Didkivska Galyna
doctor of Law, professor, head of the department
criminal law and procedure
State Tax University

Problems of criminal responsibility for criminal offenses in the field of operation-electronic computing equipment

Проблеми кримінальної відповідальності за кримінальні правопорушення у сфері експлуатації електронно-обчислювальної техніки

Studying the history of the development of crime, it is worth paying attention to one regularity, where new social relations develop, crime also appears there. According to the official statistics of the Office of the Prosecutor General of Ukraine, the number of detected criminal offenses in the field of electronic computing increased almost 7.5 times over the last year. This indicator does not take into account classic crimes involving the use of computer technology, as well as the level of latency of this type of criminal offense.

Criminal offenses in the field of exploitation of electronic computing equipment are defined as cybercrimes and are defined in the professional literature as "criminal offenses committed in cyberspace with the help of special devices (computers, smartphones, tablets, terminals and others), automated systems, computer networks or telecommunication networks, and related to illegal, unauthorized creation, storage, processing, forgery, blocking, destruction of information infrastructure objects"[1].

The latency of criminal offenses in the field of exploitation of electronic computing equipment (cybercrime) can be explained by the following features: the implementation of such a criminal offense requires a certain set of knowledge; cybercrimes, unlike other intellectual crimes, are accessible to people of low social and age capabilities; to commit cybercrimes, one does not need to occupy a high social position, it is enough to have access to the Internet and electronic computing equipment; anonymity and impersonality of cybercrimes – cyberspace identification mechanisms allow a person to use anonymously or impersonate another person, change biographical data or social status.

Considering the above, we can agree that nowadays a war in the information space can cause no less damage than a war on the battlefield. Understanding this, in the first month of the war, the parliament quickly optimized the criminal and criminal procedural legislation, improving the grounds and procedural mechanisms for bringing cybercriminals to criminal responsibility[2].

[1] Кривенко К. Кіберзлочинність: актуальна судова практика. URL: https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika

[2] Кримінальна відповідальність за кіберзлочини. URL: https://wiki.legalaid.gov.ua/

Currently, Ukraine is witnessing an increase in cyberattacks, therefore, in the conditions of war, there is a need to strengthen criminal liability.

The Criminal Code was not coordinated with the legislation in the field of cyber security and did not ensure the completeness and comprehensiveness of the investigation of cybercrimes, and the responsibility was disproportionate to the damage to the state and society.

That is why parliamentarians have optimized to counter cyber threats: 1. Art. 361 of the Criminal Code of Ukraine – cyber attack; 2. Art. 361-1 of the Criminal Code of Ukraine – creation, distribution and sale of malicious programs or techniques for cyber attacks. The Law of Ukraine "On Amendments to the Criminal Code of Ukraine on Increasing the Effectiveness of Combating Cybercrime in the Conditions of Martial Law", entered into force on 04/03/2022 (Published in the Voice of Ukraine on 03/02/2022) according to which: Art. 361 and 361-1 of the Criminal Code of Ukraine are harmonized with the legislation in the field of cyber security; in Art. 361 of the Criminal Code of Ukraine demarcated the severity of the punishment for a cyberattack depending on the consequences and increased the punishment – from a fine to 15 years in prison; search and detection of vulnerabilities is not a cyber attack (Part 6 of Article 361 of the Criminal Code of Ukraine); increased punishment under Art. 361-1 of the Criminal Code of Ukraine – from a fine to 5 years in prison[3].

Also, in accordance with the Law of Ukraine "On Electronic Communications" and the requirements of other legislation of Ukraine in the field of cyber security, the term "electronic computing machines (computers), automated systems, computer networks or telecommunication networks" was replaced by "information (automated), electronic communication, information and communication systems, electronic communication networks". The current state of affairs requires every modern socially active person in Ukraine to use mobile devices and use the Internet, state bodies conduct electronic document management, "the stable operation of financial institutions, railways and air transport, large enterprises also depends on the stability of the cyberspace with which they are forced to work, and communication is provided using electronic means of communication".

Currently, critical infrastructure facilities are also targeted. The Ukrainian provider Ukrtelecom suffered a powerful attack on March 28, 2022, during which hackers tried to analyze how the IT infrastructure is arranged, disable equipment and services, and gain control over the company's network and equipment.

On March 23, the enemy tried to carry out a cyber attack on the state institutions of Ukraine using the Cobalt Strike Beacon malware, which infects a computer if it is opened.

These are examples of massive attacks only. Probably, smaller-scale attacks and isolated cases of personal hacking are simply not reported.

We can agree that the foundations of legislative mechanisms for effective cyber defense in martial law conditions have been laid. Everyone's task is to start this mechanism

[3] Посилено кримінальну відповідальність за кіберзлочини. URL: https://capital-ukraine.com/posyleno-kryminalnu-vidpovidalnist-za-kiberzlochyny/

as soon as possible when a cyber attack is detected, so that in the future similar attacks and losses from them become less and less[4].

Taking into account the constant development of modern technologies, there is a need for constant updating of cyber protection in the sphere of cyberspace. The open invasion of the Russian Federation accelerated the improvement of current legislation and security guarantees in the modern information IT space. This, in turn, affected the issue of optimization of criminal responsibility in the field of operation of electronic computing equipment, which currently requires detailed analysis.

[4] Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix