Impact Factor: 9.2 ISSN-L: 2544-980X

Cybercrime: Concept, State, Methods of Combat

Khamdamov Golibjon Tolibjonovich [1]

Abstract: Cybercrime is an inevitable consequence of the globalization of information processes. With the growing use of information technology in various fields of human activity, their use for the purpose of committing crimes is also growing. The purpose of this study is to study the problem of cybercrime, its criminologically significant aspects necessary to assess the degree of public danger of this phenomenon, analyze the measures of the criminal law fight against it and develop proposals aimed at improving the effectiveness of the criminal law regulation of the fight against cybercrime.

Key words: cybercrime, dark net, anonymity, accessibility, methods of combat.

Introduction. We live in the era of the information society when computers and telecommunications systems cover all spheres of human and state life. But humanity, having put telecommunications and global computer networks at its service, did not foresee what opportunities for abuse these technologies create. Today, not only people, but entire states can become victims of criminals operating in the virtual space. At the same time, the security of thousands of users may be dependent on several criminals. The number of crimes committed in cyberspace is growing in proportion to the number of users of computer networks, and, according to Interpol, the growth rate of crime, for example, on the global Internet, is the fastest on the planet.[2]

Cybercrime is an inevitable consequence of the globalization of information processes. Simplicity, lightness, anonymity, accessibility, and time-saving - the qualities that make information technology attractive to mankind - could not help but attract the attention of persons engaged in illegal activities. With the growing use of information technology in various fields of human activity, their use for the purpose of committing crimes is also growing. This growth is also an inevitable process since the legislative regulation of relations in the field of information technology can neither outpace their development nor even keep pace with it.

The problem of cybercrime, due to the impossibility of being limited by the framework of one state due to its global nature, requires serious and large-scale research, as well as the development of common international standards - from the conceptual apparatus to unified legal norms.

Main part. At the XI UN Congress on Crime prevention and criminal justice, held in April 2005, special attention was paid to computer-related crime: this issue was included in the agenda and considered as part of the problem of effective measures to combat transnational organized crime.[3] In recommendations prepared for the XI Congress, UN experts speak of the special nature of cybercrime and the need to apply comprehensive approaches to combat it, as well as urgent measures to update the criminal legislation of the UN member states, such as clarifying or withdrawing norms that do not meet the current situation or the adoption of regulations relating to new types of cybercrime.

The Bangkok Declaration, which was the result of the activities of the XI UN Congress on Crime Prevention and Criminal Justice, also testifies to the urgency of the problem of cybercrime.

Unfortunately, the problem of cybercrime as a consequence of the globalization of information processes is practically not covered in the available specialized literature. This gap has yet to be filled. Several states signed the Council of Europe Convention on Cybercrime in November 2001. And if this convention is the product of a long work, that is, the world community has been concerned about this problem for more than ten years, then our country, alas, is not yet ready either to sign this convention or to international cooperation in this area. But it would be fair to mention that the international community is also still in search of not only methods to combat this problem, but also in the process of developing a unified policy on this issue, including a conceptual apparatus.

Cybercrime has an increased public danger due to the possibility of causing major damage at minimal cost and low risk. In addition, cybercrime is characterized by high latency, as a result of which law enforcement statistics do not reflect a reliable picture of the state of cybercrime both at the state level and at the global level. To assess the state of cybercrime, it

[1] Major at Bukhara regional police department, Uzbekistan

[2] Номоконов В.А. Глобализация информационных процессов и преступность. Информашйш технологи та безпека. - Кшв, 2002. - С. 98.

[3] Меры по борьбе против преступлений, связанных с использованием компьютеров. Материалы Одиннадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. A/CONF.2Q3/14. - Бангкок, 2005. - С. 25

is necessary to use other methods of obtaining data and assessing the situation: surveys, interviews, and methods of registering appeals.

Discussions and analysis. The growth of cybercrime that has occurred in recent years is noted both by law enforcement specialists of states and employees of organizations engaged in research using alternative methods of collecting statistical data. At the same time, financial losses from cybercrime amount to millions of dollars. In Uzbekistan, the growing threat of cybercrime is already recognized at the level of senior officials, who speak of it as a possible threat to the security of the state. The official statistics of our country report only a few thousand computer crimes. This problem is typical for many states. Since cybercrime is a relatively "new" type of criminal activity, and the detection and investigation of crimes are complicated by their cross-border nature, statistical data will not reflect a reliable picture of electronic attacks not only at the global level but also at the level of a single state for a very long time. The following results of our study can also be used in law-making activities to improve the criminal law on liability for cybercrimes:

- Cybercrime is understood as a set of crimes committed in cyberspace with the help of or through computer systems or computer networks, as well as other means of access to cyberspace, within computer systems or networks, and against computer systems, computer networks and computer data.
- Cybercrime is a culpably committed socially dangerous criminally punishable interference with the operation of computers, computer programs, computer networks, unauthorized modification of computer data, as well as other unlawful socially dangerous acts committed with or through computers, computer networks and programs, as well as with the help or through other access devices to the information space simulated using a computer.
- Cybercrime has a high latency (both natural and artificial, arising from the reluctance of victims to report crimes to law enforcement agencies), official law enforcement statistics do not reflect a reliable picture of the state of cybercrime both at the state level and at the global level. To assess the state of cybercrime, it is necessary to use other methods of obtaining data, such as interviews, focus groups, surveys, as well as the "case registration" method, a victimological method that consists in collecting information about cybercrime from victims. The use of these methods, along with the analysis of official statistics, makes it possible to study the scale of cybercrime and its trends, taking into account crimes that have remained outside the scope of antisocial acts registered by law enforcement agencies.
- An analysis of criminologically significant statistical data indicates the rapid growth of cybercrime, the possibility of these crimes causing significant financial damage to citizens and organizations with minimal risk to the perpetrator, as well as the growing relationship between cybercrime and organized crime. This indicates an increased danger of such acts and makes it necessary to respond to them with criminal law measures.
- The criminal law fight against cybercrime is a global problem due to the fact that cybercrime is cross-border. Therefore, in order to effectively combat cybercrime, it is necessary not only to adopt relevant criminal law norms at the national level, but also to develop common international standards, such as determining the range of acts subject to criminalization, developing a single conceptual apparatus and common terminology, revising existing criminal law norms with taking into account the standards established by international legal documents.
- The results of a comparative analysis of the legislation of the states of the world dedicated to the fight against cybercrime show that in most developed countries the following types of acts are criminalized in one form or another:

- ✓ violation of data confidentiality,
- ✓ unauthorized entry into computers and computer networks,
- ✓ encroachment on the confidentiality of information containing commercial secrets,
- ✓ Computer sabotage (intervention in functioning, modification, destruction of data, etc.),
- ✓ Economic cybercrime (particularly computer fraud).

Nevertheless, the criminalization of these acts proceeded independently of each other, as a result of which the legislation of various countries, even within the same geographical region, is very heterogeneous, the rules on criminal liability provide for various crime-forming features.

Legislative response is also required by the problem of unsolicited mailings - spam, which has now arisen for almost every e-mail user. The absence of regulations governing unsolicited mailings results in complete impunity for those involved in this activity, as well as the fact that most of the mail traffic is clogged with such correspondence. However, the proposals to criminalize this act, in our opinion, do not have sufficient grounds. It is necessary to adopt norms prohibiting spam and establishing administrative responsibility for sending it.

The growth trend of cybercrime and the trend of "lag" of social and legal control over it are linked into a kind of vicious circle, which can only be broken through an organic combination of criminal law, criminological and forensic strategies to combat this type of crime.

Conclusion. To combat the threat of cybercrime, which will certainly grow with the further expansion of the use of information technology, providing more and more opportunities for illegal activities for both individuals and criminal groups, constant international cooperation is needed. It is practically impossible to control cybercrime and fight it at the

level of an individual state. The adoption of international norms and standards should be accompanied by changes in the national legislation of states. Coordination of the efforts of states is necessary to ensure a rapid response to the development of computer technology and the adoption of appropriate regulations. Currently, more than forty countries of the world are involved in the formation of an international strategy to combat cybercrime, and this process promises to be quite long. However, despite all the difficulties, it is obvious that the international community needs to come to a solution to the problems of unifying legislation. Otherwise, given the cross-border nature of cybercrime, certain inconsistencies in legislation and uncoordinated criminal policy will allow persons who have committed socially dangerous acts to avoid liability and make it difficult to investigate crimes and prosecute offenders.

References:

1. Action Plan to Combat High-Tech Crime, Item #3, Meeting of the Justice and Interior Ministers of The Eight, December 9-10, 1997 Electronic resource.
2. Convention on Cybercrime Electronic resource. URL: http://conventions.coe.int./Treaty/en/Treaties/Html/l85.htm
3. Steering Committee for Information Technology Crime Electronic resource. URL:http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#europa.
4. Авчаров И.В. Борьба с киберпреступностью. Информатизация и информационная безопасность правоохранительных органов. XI межд. конф. -М., 2002. С. 191-194.
5. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия - Телеком, 2002. - 336 с.
6. Матвеева А. Компьютерные преступления. Человек и закон. 2002. - № 2 - С. 44 - 54.
7. Осипенко А.Л. Борьба с преступностью в компьютерных сетях: Международный опыт. — М.: Норма, 2004.
8. Сабадаш, В. Криминолого-правовая характеристика компьютерных преступлений, методика и практика их расследования. Компьютерная преступность и кибертерроризм. Исследования, аналитика. Вып. 2. Запорожье, 2004. - С. 167 - 173.