IQRO JURNALI / 2023
GUVOHNOMA № 060680
E-ISSN : 2181-4341
https://wordlyknowledge.uz
IMPACT FACTOR(SJIF) : 3,934
Volume 3 issue 2 - 2023

CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY

Gapparova Sevara Khikmatulla qizi

Student of Karakalpak State University named after Berdaq

Annotation

This article will reflect the origin of crimes in the field of Information Technology, their types, criminal justice description, solve their qualification tables, and provide legal and organizational and technical advice on the Prevention of such crimes.

Keywords

Theft, cyber thieves, hacker, crimes and their types in the field of Information Technology, the object, subjective side and subject of crimes in the field of Information Technology.

The modern world is developing rapidly. This is due to the fact that advances in science and technology interpret more favorable opportunities for our daily social life. However, along with similar advantages and amenities, there are also some negative situations. As we all know, there is a negative concept that goes against the ethical rules of theft. Theft means the secret looting of one's property. Sometimes we can hear about some kind of bank mess, such as the fact that the store is overnight. Indeed, theft is among the bad vices that cause great harm to society as a whole. There are also such robberies in our lives that it is completely different from the usual robberies. As well as being carried out by highly intelligent, agile individuals, such robberies tend to be extremely cunning. While it is 10-20 times more difficult to identify such thieves, as well as their prints, than to identify ordinary thieves, it is easy to calculate the damage they caused. Another interesting thing is that they never move as a team. Self – reproduction is possible only when one goes to work alone and then enters the theft area. Intrude and wander into other people's “houses” without permission, and do not always leave without any harm. Such thieves are called cyber thieves in the world of the internet. Cyber thieves are computer viruses and hackers who infiltrate computer memory and carry out their infamous intentions. Individuals who commit cyber theft are referred to as hackers, and the word “hacker” is derived from English, Meaning “Hack” to crack, run, break. Who is the hacker himself? As you know, a person who is a strong specialist in any field cannot be considered to possess good properties, there is a saying in our people “if you are a scientist, the universe is yours”, but there are wise words about those who do not spend this acquired knowledge in the interests of mankind, but also seek negative paths in their own interests.

Unfortunately, the more information technology has evolved globally, the more professional hackers have become available. 80% (percent)of users in the computer world consider hackers – criminals. As a result of the constant development of Information Technology and the emergence of the internet, the concept of “crimes in the field of Information Technology” has entered. Crimes in this area can be committed in two ways. If they are using a computer that is computer crimes, it is referred to as cybercrime if it is committed over the internet. A crime in the field of information technology is a criminal offense committed using computer and data processing systems. Of course, the legislation provides for liability for this act.

Some types of crimes in the field of information technology can be seen in:

Google Scholar ADVANCED SCIENCE INDEX ResearchGate OpenAIRE zenodo doi digital object identifier

* Viral software distribution;

* Theft of user confidential information;

* Stealing other people's intellectual activity products;

* Hacking other people's accounts on social networks;

* Spread false information, stop;

• Inciting inter-Millar conflict and inter-religious animosity;

* Illegal transactions with Bank plastic cards (card details ;

• Securities market internet fraud;

* Financial pyramids on the internet;

* Crimes related to mobile communications;

• Other crimes in the field of e-commerce.[1]

For the most part, lack of legal knowledge about crimes in this area and the fact that citizens with computer offenses do not turn to law enforcement agencies also create complexity in exposing crimes. At this point, the Russian scientist, it is permissible to cite the following points of Sorokin, “accepting that information is also a tool in committing other crimes complicates the work of both the Legislature and the rightsholder in over-expanding the scope of the concept of” Computer Crime”".[2]

The law of the Republic of Uzbekistan dated December 25, 2007 “on amendments and additions to certain legislation of the Republic of Uzbekistan in connection with increased liability for illegal actions in the field of informatization and data transmission”, taking into account such cases, defined dangerous acts related to the use of computer systems as crimes and supplemented the current criminal code with Chapter XX1 “crimes in the field of Information Technology”. This chapter is included in the sixth chapter of a special part of the Criminal Code called “crimes against public safety and public order”, which includes the following articles:

- P. 2781. Violation of informatization rules;

- P. 2782. Illegal (unauthorized) use of Computer Information;

- P. 2783. Preparation or transfer and distribution of special tools for the illegal (unauthorized) use of a computer system, as well as telecommunication networks;

- P. 2784. Computer information modification;

- P. 2785. Computer sabotage;

[1] http://naveconomy.uz

[2] Sorokin A.V. Computernie prestuplenia: ugolovno-pravovaya characteristic, methodology I Praktika rascritia I rassledovania. Resource Internet: //http://kurgan.unets.ru/-procur/my_page.htm, 1999.

- P. 2786. Create, run, or distribute malicious programs;

- P. 2787. Illegal (unauthorized) use of a telecommunications network.

Particular attention should be paid to the composition of the crime in the qualification of crimes in the field of Information Technology. The object of this crime is, according to some views, social relations regarding the legal and safe use of Information Technology, the objective side of action is committed through inaction. As an example, if the objective side of the crime of violation of the rules of informatization of Article 2781 is reflected in the significant damage to the rights of citizens or the law-guarded interests or the state or public interest as a result of the creation, implementation and use of information processing and its transmission systems without taking established protective measures, - the objective side of the crime provided for by the article is characterized by the illegal (unauthorized) use of computer information, which causes the destruction, blocking, modification, copying of information or its capture, violation of the work of electronic computing machines, electronic computing machines system or their networks Mascur as for the subjective side of the crime, it is characterized by a Only one of the above crimes, that is, a crime in Article 2781 of JK, which establishes liability for violations of the rules of informatization, can be committed both intentionally and carelessly. the purpose is set by the Legislature for two crimes of the JC, sections 2783 and 2786, as a necessary sign of the subjective side of the crime. And in the rest, the motive and purpose are not indicated as a necessary sign, but their designation is of great importance for the individualization of punishment. These crimes are intended for the purpose of greed, bullying, revenge. It is committed in the motive of political and other interests.

Based on the analysis of objective and subjective signs, these crimes are defined by legal scholars as: “a socially dangerous act that carries the risk of harm or harm to social relations in the legal and safe use of computer information is called crimes in the field of Information Technology” [3]

The subject of Information Technology crimes are sane, persons who are 16 years old, have a duty to guard information, or are illegally accessing computer information.

In order to protect internet users from possible illegal offenses from crimes committed in the field of information technology, some recommendations have been made, which include: security-responsive updates are installed, the use of an operating system with current versions of other software, the need to pay attention to their appearance, web addresses when using sites, the need to include personal data, it is important not to use passwords that are very easy and light to find and use with similar precautions.

From the above, it is worth noting that the protection of citizens from crimes committed in the field of Information Technology or the Prevention of their occurrence is an important issue. The best way to protect citizens from crimes in the field of information technology is to become aware of modern threats, therefore, it is necessary to study, disseminate information about such threats and carry out propaganda and propaganda work. After all, the safety of all of us is in our hands.

[3] Kabulov R.K., Abdurakhmanov E.S. Crimes in the field of Information Technology: a study guide. - T.: Academy of the Republic of Uzbekistan, 2009. – 15 b.

Google Scholar ADVANCED SCIENCE INDEX ResearchGate OpenAIRE zenodo doi digital object identifier

List of used literature

1. http://naveconomy.uz
2. Sorokin A.V. Computernie prestuplenia: ugolovno-pravovaya characteristic, methodology I Praktika rascritia I rassledovania. Resource Internet: //http://kurgan.unets.ru/-procur/my_page.htm, 1999.
3. Kabulov R.K., Abdurakhmanov E.S. Crimes in the field of Information Technology: a study guide. - T.: Academy of the Republic of Uzbekistan, 2009. – 15 b.

WORDLY
KNOWLEDGE