CRIMES IN THE FIELD OF INFORMATION TECHNOLOGIES AND METHODS OF PROTECTION AGAINST THEM

Tokhtaev Anvar Ilhamovich
Main Department of Internal Affairs of Tashkent city
Deputy head of the department for combating
crimes in the field of information technologies, Lieutenant colonel

Abstract. This article talks about crimes in the field of information technology and ways to protect against them. The large-scale development of information technologies has made it possible to commit many types of crimes at the same time, and in turn, detection and prevention of these types of crimes require high knowledge and professional training.

Key words: crimes, information technologies, protection methods, information system, Internet, electronic crimes.

Annotatsiya. Ushbu maqolada axborot texnologiyalari sohasidagi jinoyatlar va ulardan himoyalanish usullari haqida so`z yuritilgan. Axborot texnologiyalarining keng ko'lamli rivojlanishi bir vaqtning o'zida ko'plab turdagi jinoyatlarni sodir etish imkonini berdi va o'z navbatida bu turdagi jinoyatlarni aniqlash va oldini olish yuqori bilim va kasbiy tayyorgarlikni talab etadi.

Kalit so`zlar: jinoyatlar, axborot texnologiyalari, himoyalanish usullari, axborot tizimi, internet, elektron jinoyatlar.

Абстракт. В данной статье говорится о преступлениях в сфере информационных технологий и способах защиты от них. Масштабное развитие информационных технологий позволило совершать одновременно множество видов преступлений, а в свою очередь раскрытие и предотвращение этих видов преступлений требуют высоких знаний и профессиональной подготовки.

Ключевые слова: преступления, информационные технологии, методы защиты, информационная система, Интернет, электронные преступления.

In the conditions of global development, finding more modern, innovative ways to increase the essence of information technologies, providing comprehensive support to the process of information and widely introducing them into life is becoming one of the important directions of state activity. After all, the issue of conducting state policy in the information system is a task of strategic importance.

Today, the rapid development of information technologies and the widespread use of the Internet in all spheres of human society have become a part of daily activities and have entered service, science, education, e-commerce, as well as the way of thinking of a modern person with its positive influence. In addition to these changes related to the improvement of the quality of life, it should be noted that favorable conditions for the development of new forms of crime have appeared.

These crimes, in turn, are called "Crimes in the field of information technologies" (electronic crimes).

The large-scale development of information technologies has made it possible to commit many types of crimes at the same time, which, in turn, requires high knowledge and professional training in the detection and prevention of these types of crimes.

Thus, "crime in the field of information technology" is a criminal act committed using computers and data processing systems, for which criminal liability is provided by law.

Therefore, it is necessary to disseminate information about crimes in the field of information technologies among citizens and carry out propaganda work.

With the continuous development of information technologies and the emergence of the Internet, the concept of "crimes in the field of information technologies" was formed. The main difference between electronic crimes is that some of them are committed using a computer (computer crimes), while others are committed over the Internet (cybercrimes).

Forms of electronic crime are multifaceted and are increasing with the continuous development of technology and the Internet. Also, there are a number of difficulties in detecting and exposing these crimes, one of which is due to the reluctance of citizens to report computer crimes committed against them to law enforcement agencies and insufficient legal knowledge when faced with computer crimes.

Some types of IT crimes can be seen in:

- distribution of virus software;
- steal user's confidential information;
- stealing other people's intellectual activity products;
- hacking other people's accounts on social networks;
- spreading false information, defamation;
- inciting inter-ethnic conflict or inter-religious enmity.
- illegal transactions with bank plastic cards (card details);
- Internet fraud in the stock market;
- Financial pyramids on the Internet;
- crimes related to mobile communications;
- other crimes in the field of electronic commerce.

Taking into account the above examples, some recommendations can be made for Internet users to prevent illegal offenses that may be committed against them:

- -access the Internet, use devices with special software designed to combat malicious activity, update them on time;
- - use an operating system with security updates installed, current versions of other software;
- - when using sites, pay attention to their appearance, web address: maybe you have entered a fake copy of it;

• - enter personal data only on websites that use secure protocols (usually a block icon is displayed on a green background next to the address of such a site in the browser);

• - do not use the same login and passwords on different sites;

• - do not use very light or easily guessed passwords (date of birth, phone numbers, etc.);

• - whenever possible, use two-factor authentication, which requires entering a temporary code in addition to entering a username and password, usually sent to your mobile phone in the form of an SMS message or a "PUSH" notification;

• - beware of unexpected or unusually random e-mails, even if you know the sender, never open attachments or use links in such e-mails;

• - beware of e-mails that require credentials (financial institutions almost never ask for financial information via e-mail), never send financial information through unsecured Internet channels;

• - when you receive messages from friends encouraging you to carry out financial transactions or transfer financial information, verify this information using other communication channels (personal meeting, phone call, messenger with the ability to send voice messages) or, in extreme cases, by asking control questions whose answers cannot be known by third parties specify the identity of your interlocutor;

• - When making payments via the Internet, if possible, use additional payment security technologies such as "3D Secure" for international payment systems "Visa" and "MasterCard";

• - never talk on the phone with strangers who introduce themselves as bank employees and ask you to give your bank card information;

• - keep your bank card information in a safe place, do not tell anyone, message or send them via SMS, etc.;

• - limit your circle of friends and loved ones to save your records. Never share your personal information with new online friends. Avoid publicizing information such as dates of birth, email addresses, or pet names that could be used as passwords. All this information can be very useful for a professional hacker;

• - "Attention! Your account has been hacked. You must call to verify your account. Be wary of messages like "message us and we'll call you back";

• - Don't become a victim of "click jacking". This is a type of cyber attack that contains hyperlinks that at first glance appear to be harmless content. However, clicking on the hyperlink opens the way for malicious software, which can attack your computer or transmit your personal information;

• - In email addresses and on the website, carefully review the URLs, even if they contain the names of reputable financial institutions that you do business with. The most common scam is a combination of a legitimate website name and a fake one. These addresses often lead to copycat sites that disguise their involvement in hacking activities under the guise of being legitimate. Sometimes the URL may be legitimate, but when you click on the link, it will take you to another site.

Based on the above, in conclusion, it should be noted that the best way to protect against crimes in the field of information technology is to be aware of modern threats.

References

1. Constitution of the Republic of Uzbekistan.
2. Law of the Republic of Uzbekistan "On Information".
3. Law of the Republic of Uzbekistan "On Electronic Government".