Sulaymonova Yulduz Izzatulla qizi
Jahon iqtisodiyoti va diplomatiya universiteti magistranti. Adliya vazirligi huzuridagi Huquqiy siyosat tadqiqot instituti katta maslahatchisi

AQSHDA AXBOROT TEXNOLOGIYALARI SOHASIDA JINOYATCHILIKGA QARSHI KURASHISHNING DOLZARB MUAMMOLAR

Sulaymonova Yulduz Izzatulla kizi
Master`s student of Universiteti of world economy and diplomacy. Consultant of the Research Institute of Legal Policy under the Ministry of Justice.

ACTUAL PROBLEMS OF COMBATING CRIME IN THE FIELD OF INFORMATION TECHNOLOGY IN THE UNITED STATES

Сулаймонова Юлдуз Иззатулла кизи
Магистрант Университета мировой экономики и дипломатии. Старший консультант Исследовательского института правовой политики при Министерстве юстиции.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В США

One of the most pressing problems of the world community has been the exponential growth in the last decade of crimes in the field of information technology. The availability of personal computers with the most powerful processors, the presence of the Internet in almost all spheres of human activity, millions of gigabytes of content about ways and methods of hacking networks, the enormous growth in sales of smartphones, tablets and other fashionable gadgets in recent years create new real threats to society.

Crime in the field of information technology has no territorial borders, is characterized by high latency, the damage from its actions amounts to hundreds of billions of dollars, and the level of detection of these crimes is negligible. Cyberterrorism, fraud, extortion, hacking of secure networks, distribution of counterfeit, pornographic products, malware, "digital drugs", carding – from the English carding, fraud with payment cards) – this is a far incomplete list of crimes committed by intruders in the field of information technology. In addition, the vast majority of life support enterprises, energy, chemical, and oil and gas industries are managed and controlled by computer systems, and the consequences of hacking and disrupting the operation of such systems cause reasonable public concerns.

The first bill establishing criminal liability for crimes in the field of information technology was developed in the United States back in 1977. Based on this bill, the Computer Fraud and Abuse Act (CFAA) was passed in October

1984 – the main regulatory legal act establishing criminal liability for crimes in the field of computer information. Subsequently, it was repeatedly supplemented.

The Law on Fraud and Misuse of Computers establishes responsibility for several main crimes: computer espionage; unauthorized access to information; computer fraud; intentional or negligent damage to protected computers; threats, extortion, blackmail committed using computer technology and others.

The US government recognizes the seriousness of the problem of cyber crime for both the public and private sectors, and has taken serious steps to combat this type of cyber threat. To combat crimes that exploit the opportunities provided by the freedom of movement of goods, services, data and capital via the Internet, in 2006 the United States ratified the Council of Europe Convention on Combating Cybercrime (known as the Budapest Convention), becoming the 16th state to ratify it.

The Budapest Convention entered into force in 2007. Within the framework of the Convention, the United States supported the processes of international harmonization of substantive and procedural legislation in the field of combating cyber crime by creating an informal channel for collecting and exchanging information among the G7 countries, round-the-clock contact points and coordinating the efforts of donor countries in assisting developing countries. In addition, US law enforcement agencies regularly cooperate with a large number of partner countries in the arrest and extradition of criminals for their prosecution in the US or other countries.

The Cyberspace Policy Review of 2009 identified more than 90 legislative acts that need to be improved to meet modern realities. Since 2009, several bills in the field of cyber security have been presented at each session of the Congress, but only a few of them have received the support of both factions and have become laws. One of these laws was the "Cyber Security Act of 2015" (CSA), which was included in the Consolidated Appropriations Act for 2016 (Consolidated Appropriations Act). The CSA establishes a process for exchanging information about cyber threats between government agencies, as well as between them and business organizations that voluntarily agree to participate in the program. Some of the provisions of this Act turned out to be necessary for the Department of Justice and the Federal Trade Commission to confirm the validity of the 2014 decision that the exchange of information about cyber threats with competitors is not a violation of anti-trust legislation. Taking into account that the decision and approach of the Ministry and the Commission cannot eliminate all the possibilities of abuse (for example, market collusion), the CSA includes provisions on liability protection for certain types of information about cyber threats. Currently, there is a large list of US legislative acts that need to be revised and improved in order to expand the capabilities of law enforcement agencies and enable the public to protect their country, and the country to fully establish cooperation with other states in order to reduce criminal activity.

In the more recent past, influential senators from the Republican and Democratic parties announced the creation of a non-partisan "Senate Cyber Bloc (parliamentary Group)", which could serve as a platform for a comprehensive and unbiased consideration of cyber issues, and would also allow senators and their staff to be fully informed on cyber policy and legislation. Among the main topics on which the work of the new block will focus are the impact of cyber crime on national security and the economy, as well as ways to deprive criminals of opportunities to escape punishment using modern technologies. The US House of Representatives created similar, but partisan mechanisms in 2011, when the leadership of the Republican Party created an operational group to study cyber security issues in the areas of work of all parliamentary groups. This group identified at least sixteen laws that needed to be reformed and published a list of legislative recommendations.

Back in 2008, as part of the Comprehensive National Cybersecurity Initiative (CNCI), former President George W. Bush decided that the Department of Justice and the FBI would be "the leading organizations in the field of investigation of cyber crimes and prosecution of criminals". To implement this task, the Joint National Cyber Research Task Force (NCIJTF) was created, which continues to serve as the national coordination center for cyber risk investigations and research. In its role as a joint interagency committee, NCIJTF develops cooperation and organizes joint operations with the participation of federal intelligence and law enforcement organizations that are directed against cyber terrorists who exploit flaws in critical infrastructure control systems; theft of intellectual property and trade secrets at the state or country level; criminals who commit theft of financial resources or personal data, or other cyber data; hackers who illegally break into the systems of commercial or government organizations; as well as insiders who commit theft and acts characterized as sabotage. Recently, the Department of Justice and the FBI have increased funding for cyber security activities by 23% to increase the capacity to detect, prevent and neutralize malicious cyber attacks.

The FBI has also created a specialized Cyber Division (CyD), which implements its activities using NCIJTF resources and coordinates the work of special cyber teams in 56 regional offices throughout the United States. The staff of these offices includes agents and analysts who investigate cases of cyber attacks, theft of data and intellectual property, as well as personal data; cases of illegal exploitation of children and the distribution of child pornography, as well as cases of online fraud. Many of these investigations have led to the destruction of botnets, the criminal prosecution of international criminal groups, as well as the creation of analytical reports on the latest trends in the development of malware. CyD is also actively involved in cooperation with international partners through a number of mechanisms, including programs for the introduction of positions of Legal Attache and Legal Attache on Cyber Issues (Legal and Cyber Assistant Legal Attaché); The recently established International Cyber Crime Coordination Cell, located in the CyD office at the FBI;

the international internship program at the National Cyber Forensics and Training Alliance (NCFTA) in Pittsburgh; participation in bilateral and multilateral investigations; as well as delegation of officials to international cyber centers in Europol and Interpol.

The US Secret Service has also created a special structure for the investigation of electronic and financial crimes. The Secret Service has created a Task Force on Electronic Crimes, working on a national and international scale, the main purpose of which is to detect and identify cyber criminals associated with criminal activities in cyberspace, bank fraud, database hacking, as well as other crimes in the IT sphere. Cyber Intelligence Section the Secret Service was directly involved in the arrest of international cyber criminals responsible for the theft of hundreds of millions of credit card numbers and the subsequent theft of more than $ 600 million from the accounts of financial and trade organizations. In addition, the Secret Service is the founder of the National Computer Forensic Institute, which provides training and information on combating cyber crime to law enforcement officers, prosecutors and judges.