Vladimir Golubev
Crime-research.org

Fighting computer crimes in Ukraine

The global informational civilization has defined information as its base parameter – publishing business, press, radio, TV, computer technologies, other means of electronic communication became leading factors of the economic, industrial, scientific, educational, political and other fields of social activity. It means that different information systems and telecommunication networks are an intensifying factor of the society and state. Information society does not simply change the status of information (information, knowledge, and data) as a catalyst of positive changes in the social being but also widens possibilities of delinquent groups to use information for the antisocial purpose [1].

These tendencies can be watched all over the world and Ukraine is not an exception. Spread of computer viruses, fraud with plastic payment cards, drawing money from banking accounts, theft of computer information and violation of computer system operating rules are some of computer crimes. That is why there is an urgent problem of counteracting them both in Ukraine and many other countries through out the world. Such crimes have tendencies to become aggravated. They are already a definite social danger that threatens information security – a component of national one. According to experts, this phenomenon presents a more serious danger than five years ago due to the use of the latest information technologies and high vulnerability of up-to-date industrial society. In spite of efforts directed by many countries to fight cybercrimes, their number constantly increases in the world.

Problems of researching computer crimes and developing procedures of their investigation are of particular interest to the scientists. P.Bilenchuk, V.Gavlovsky, N.Gutsalyuk, R.Kalyuzhny, V.Tsymbalyuk and other authors deal with theoretical and practical aspects of computer crimes and legal regulation of information traffic in Ukraine. The topical character of such researches is stipulated by demand of law enforcement practice for scientifically based recommendations on fighting and investigating computer technology crimes.

The example of large-scale computer robbery in 1999 can prove the serious character of this problem [2]. 80,4 million UHR ($20 million) were drawn from the reserve fund of Ukraine's National Bank in Vinitsa by obtaining unauthorized access to the banking computer network. Eight months later, the mafia fighting service succeeded in arresting more than thirty persons involved in committing this resonance crime after conducting eleven preplanned searches.

Russian hackers are accused of stealing Microsoft secret codes, downloading information from Pentagon computers, cracking NATO web sites, drawing thousand numbers of credit cards through Internet and million dollars from West banks.

For the first time Russian hackers attracted attention of the whole world when in 1994 Vladimir Levin, a young mathematician, cracked Citibank computers and transferred twelve million US dollars to the banking accounts of his friends in different countries of the world. He handled this operation staying at Saint-Petersburg apartment. Finally, he was found and arrested but the other hackers went on demonstrating their skills in committing cybercrimes.

The case became widely known in the press when Russian law enforcement bodies rendered harmless the criminal group that had succeeded in penetrating into American large online shop handling business through Internet. The criminal case materials run: "…in February 1998 Ilya Hoffman, the viola student of Moscow conservatory, found Authorise software in Internet that offsets between shops and plastic card holders when ordering and purchasing products through Internet. He downloaded that program to his computer thereby obtaining an access to information on numbers of plastic cards, which help to pay for products in "computer" shops [3]. The mechanism of swindle consisted in that when staying at home and operating in Internet, Hoffman imitated the work of Virtualynx Internet LLC online shop (Vancouver, USA) that accepts orders for products and receives payment for them through Internet. He acted as a salesclerk and buyer at the same time. When pretending to be a purchaser, he supposedly ordered products paying for them at the expense of funds on the plastic cards, account numbers of which he learned from Authorise program. The legal keepers of cards did not even suspect that they "bought" something in Vancouver. After effecting such a transaction, Hoffmann canceled an order. However, he indicated the number of "false" card belonging to an accomplice. Hoffman's accomplices opened banking accounts in advance. The criminal could not transfer money from card to card, because such an operation would have been noticed at once. In conclusion, the delinquent persons drew funds from the online shop account and put them to the account of an accomplice's "false" plastic card. Ilya Hoffman was arrested on the charge of stealing $97 000 through Internet.

According to experts, now every hacker drawn dollar accounts for that invested in the computer security. Any housewife heard something about hackers but few persons know about those who create the defense system to fight computer criminals. This invisible struggle continues all the time: a new protecting technology (patch) is developed to suppress every new cyberattck.

The experts in banking fraud warn that hackers from former USSR countries present the most serious danger for the bank security. Unfortunately, computer crimes are not regarded as something serious because law enforcement agencies have many other problems in addition. A lost credit card is considered nothing in comparison with murders and other crimes committed in the country.

To make it clear for an ordinary person how great the danger of a hacking attack is, the experts explain: any crime now (except rape) can be committed by using a computer, even a murder. Just imagine the penetration into the medical center network where the patients with artificial heart and other life-support organs are connected to the computer system; or cracking the chemical plant server: once the technology is changed, the mass poisoning of people becomes quite real.

The e-commerce, banks, Internet-shops, through which the criminals try to obtain clients' passwords and codes, can be referred to the group of risk. For example, the following situation occurred in one of the large Russian Internet-shops "Ozon". According to Georgy Ushakov, Technical Director, every day Ozon computer security system faces in average up to one hundred attempts of penetration, most of them being automatically repelled by the installed program means. Additional actions of the system are required to repel 10-15 attacks. Once or twice a week, the shop is attacked in a nonstandard way. The experts in computer security have to be enlisted in those cases. The hackers attacking Internet-shops in general and "Ozon" in particular pursue the following objects:

1. Location of supposedly paid orders in the shop system;

2. Full or partial interruption of the shop operation;

3. Replacement of the site contents.

In April 2003, US law enforcement bodies arrested about 130 persons during the operation on revealing crimes committed through Internet. More than $17 million were confiscated within the framework of that operation. According to US Minister for Justice, the operation results prove the necessity of fighting these crimes because Internet gives the criminals an opportunity to act in an anonymous way. More than 89 thousand complaints were examined during the operation. The damage made up $176 million.

Helkern computer worm attacked Internet early 2003. It caused losses of some billion US dollars.

Unfortunately, Ukraine knows some cases of spreading computer viruses in its information resources and receiving undesirable e-correspondence through Internet. In this connection, the State should urgently solve the problem of protecting computer systems and networks as a part of the national infrastructure, introducing changes into laws that regulate questions of fighting computer crimes, and creating an appropriate joint center provided by Ukraine's President Decree of December 6, 2001 [4].

Certainly, there is still no universal remedy for such a disease as "hacking" and "cracking" but Computer Emergency Response Team (CERT) can be used as a vaccine. Many small and big CERT groups act now in different countries. They work at large academic networks, organizations with the sophisticated broad network and banks as well.

One of the most serious problems nowadays is an increase in number of computer crimes. Every computer network is a potential target for cyberattacks. Cybercrimes are known to be committed practically every day. In this connection, especially significant are the legal regulation and international cooperation in fighting transnational computer crimes.

In spite of economic difficulties, Ukraine's Internet segment has a dynamic development. According to experts, every six months the number of hosts in UA segment increases in average by 1.7 thereby exceeding the average rate of Internet growth as a whole. Ukraine takes the first place among East Europe countries by the number of Internet providers [5]. According to different research companies, the total number of Internet users in Ukraine is ranged from 600 to 950 thousand early this year.

Therefore, the problem of fighting computer crimes in Ukraine should be solved today as tomorrow it can be too late. The analysis of home laws regulating social information relations allows affirming that our State takes necessary steps of fighting computer crimes and those of stimulating the development of the latest technology-based infrastructure. Ukraine's President Decree "Measures of developing national component of Internet and providing a broad access to it in Ukraine" of July 31, 2000 [6] and Ukraine's new Criminal Code Section 16 "Crimes committed by using electronic computers, systems and computer networks" [7] can serve as an example of it.

On April 3, 2003, Ukraine's Parliament accepted the law "Introduction of changes into Ukraine's Criminal Procedural Code" that will make it possible to widen Ukraine's Security Service possibilities when investigating disruptions in the work of automated systems.

The international experience can also prove the necessity of using special services in fighting computer crimes. For example, in USA, National Security Agency and its Computer Security Center deal with such matters, except FBI. In France, Security Service is engaged in it, in addition to Special Police Brigade. The same situation is in Canada.

The participation of Security Service in preventing, revealing and exposing crimes provided by Articles 361, 362 and 363, Ukraine's Criminal Code, and use of its resources and possibilities are necessary to create an effective system of counteracting computer crimes in Ukraine.

According to Ukraine's Security Service officers, this law does not provide for monitoring information in Internet but bears a practical character that will allow Security Service to protect national interests in a more effective way.

It would be important for Ukraine to create a special team (CERT-UA) responding on transnational computer incidents and mass counteraction to such cybercrimes. Information networks in Ukraine and other countries can suffer in the near future without such a team (-s).

In conclusion, I want to emphasize that the problem of fighting computer crimes is a complex one. Today the law must meet the requirements raised by the modern level of technology development so that the justice can be administered independently of means used to commit a crime (usual ones or Internet and personal satellite connection). The priority direction is to organize interaction and coordinate efforts of law enforcement bodies, special services and court system, supply them with required material and technical base. No State is capable of opposing this evil without help today. It is necessary to intensify the international cooperation in this field. There is no doubt that the important place in this cooperation belongs to the internationally legal mechanism of regulation.

1. R.Kalyuzhny, R.Kolpak “Mafia’s use of information technologies to influence the society”. - Fighting mafia and corruption (theory and practice) // Scientific and practical magazine. - ¹3. – 2001. – P.160.2. Internet news agency.

3. Dragon from Internet // Art-Mosaic. - ¹49. – 1999.

4. Ukraine’s President Decree of December 6, 2001 “Ukraine’s National Security and Defense Council Decision of October 31, 2001”Measures of improving State information policy and providing information security in Ukraine”.

5. Vitalie Balyuk. Today’s Ukrainian Internet segment. - http://boy.dlab.kiev.ua/PRJ/B_Int/Main/Addon/Lib/anal_ukr.htm.

6. Ukraine’s President Decree “Steps of developing national component of Internet and providing a broad access to it in Ukraine” of July 31, 2000. - http://www.crime-research.org/library/Ukaz_Inter.htm.

7. Ukraine’s Criminal Code of April 5, 2001. – K., Ukraine’s official bulletin, 2001. – P.105-106.