12. Domestic code of Ukraine : Law of Ukraine dated January,10,2002 № 2947 – III, List of Verkhovna Rada (2002), № 21 – 22, article 135.

13. Chmut S.V. (2006) "Zlochinni dii pri statevih znisinah z osoboyu yaka ne dosyagla statevoyi zrilisti", *Criminal acts at carnal knowledge with a person that did not come to sexual maturity*, Criminal-legal politics of the state : theoretical and practical aspects of problem : Proceedings of International scientific conference, Donetsk, dated November, 17–18, 2006, Donetsk Law Institute of Internal Affairs of Ukraine, pp. 282-287.

УДК 351.749: 343.451 (100)

TOPICAL ISSUES OF THE ESTABLISHMENT AND FUNCTIONING OF SPECIAL STATE ORGANIZATIONS TO FIGHT AGAINST THE INTERNET FRAUD IN DIFFERENT COUNTRIES OF THE WORLD

Sabadash V.P., candidate of law, associate professor

Zaporizhzhya national university (sabvp@mail.ru)

The article deals with topical issues of combating online fraud by analyzing the activity of the state special organizations of such leading countries of the world as the USA, Great Britain, Russia, France, Germany and some other countries, that have gained an extensive experience in the establishment and functioning of such departments and organizations which can be used for creating similar services in other countries.

Key words: Internet fraud, fight, prevention, special department, special organization, investigation, crime, cybercrime, information technology.

Сабадаш В.П. АКТУАЛЬНЫЕ ВОПРОСЫ СОЗДАНИЯ И ФУНКЦИОНИРОВАНИЯ ГОСУДАРСТВЕННЫХ СПЕЦИАЛЬНЫХ ОРГАНИЗАЦИЙ ПО БОРЬБЕ С ИНТЕРНЕТ-МОШЕННИЧЕСТВОМ В РАЗЛИЧНЫХ ГОСУДАРСТВАХ МИРА / Запорожский национальный университет, Украина

В статье рассматриваются актуальные вопросы противодействия интернет-мошенничеству путем анализа деятельности государственных специальных организаций таких ведущих стран мира, как США, Великобритания, Российская Федерация, Франция, Германия и некоторых других стран, в которых накоплен огромный опыт по созданию и функционированию таких подразделений и организаций, который можно использовать при создании аналогичных служб в других странах мира.

Ключевые слова: интернет-мошенничество, борьба, противодействие, специальные подразделения, специальные организации, расследование, преступление, киберпреступность, информационные технологии.

Сабадаш В.П. АКТУАЛЬНІ ПИТАННЯ СТВОРЕННЯ ТА ФУНКЦІОНУВАННЯ ДЕРЖАВНИХ СПЕЦІАЛЬНИХ ОРГАНІЗАЦІЙ ПО БОРОТЬБІ З ІНТЕРНЕТ-ШАХРАЙСТВОМ У РІЗНИХ ДЕРЖАВАХ СВІТУ / Запорізький національний університет, Україна

У статті розглядаються актуальні питання протидії інтернет-шахрайству шляхом аналізу діяльності державних спеціальних організацій таких провідних держав світу, як США, Великобританія, Російська Федерація, Франція, Німеччина та деяких інших держав, у яких накопичено великий досвід щодо створення та функціонування таких підрозділів та організацій.

Однією з особливостей створення таких державних спеціальних організацій є те, що вони створюються державами у складі центральних органів влади: Міністерств, відомств, Служб безпеки тощо. Так, у Російській Федерації – це Бюро спеціальних технічних заходів МВС Росії, до структури якого увійшло Управління «К».

У Великобританії питаннями боротьби зі злочинами у сфері високих технологій до останнього часу займалося Національне Агентство по боротьбі з організованою

злочинністю (SOCA). На сьогоднішній день SOCA (як аналог ФБР США) є самостійним (організаційно незалежним) міжвідомчим державним правоохоронним органом уряду Об'єднаного Королівства, що формально віднесений до Міністерства внутрішніх справ, який здійснює свою діяльність у межах усього Об'єднаного Королівства та співпрацює (через його мережу міжнародних представництв) з багатьма зарубіжними правоохоронними органами та спецслужбами. З 1 жовтня 2013 року функції SOCA в частині боротьби із комп'ютерною злочинністю передані Національному підрозділу протистояння кіберзлочинам Національного агентства по боротьбі зі злочинністю.

Важлива роль у протидії шахрайству Великобританії відводиться також спеціальному управлінню Королівської прокурорської служби, а саме – Центральній групі з протидії шахрайству, спеціалісти якої фокусують свої зусилля на підтриманні обвинувачення у справах про великі й складні шахрайства.

Найбільш розгалужена система державних спеціальних організацій щодо протидії інтернет-шахрайству існує у Сполучених Штатах Америки, де питаннями боротьби зі злочинами у сфері високих технологій займаються декілька спеціальних державних організацій. По-перше, це Федеральне бюро розслідування (FBI), у складі якого у 1996 році створено Кіберпідрозділ (Cyber Division FBI). Крім того, у складі Міністерства фінансів США діє Секретна служба США (US Secret Service), яка проводить розслідування фінансових злочинів за декількома напрямками фінансової направленості.

Розглянуто також особливості функціонування державних спеціальних організацій в інших державах світу, таких, як Франція, Німеччина, Канада, Індія.

Досвід створення таких організацій безперечно можна використовувати при створенні аналогічних служб в інших державах світу.

Ключові слова: інтернет-шахрайство, боротьба, протидія, спеціальні підрозділи, спеціальні організації, розслідування, злочин, кіберзлочинність, інформаційні технології.

Today a variety of high-tech devices are used in everyday life – plastic cards, mobile phones, tablets and computers. New models, programs and services are being developed. All these things make our lives better, but they require certain skills and knowledge. Modern society has become more technologically dependent.

However, along with development of high technologies, new types of fraud aimed at appropriation of citizens' funds are coming into existence. This, in its turn, sets tasks of combating such fraud actions by the society and law-enforcement bodies. In particular it concerns the global Internet, which knows no borders and allows fraudsters to carry out their criminal plans at a distance. Even a new term "online fraud" has come into use.

So, the purpose of this article is to research the issues of establishment and functioning of special units combating the Internet fraud in different countries of the world with the aim of borrowing the accumulated experience of law-enforcement and non-governmental organizations' activities.

Having studied the scientific issues of the problem of combating the Internet fraud by the establishment of special units to fight against such criminal actions we have come to a conclusion that no special research of these issues has been made at present stage. However, it should be noted that some aspects of fighting against computer crimes have been considered by D.S. Azarov, J.G. Baturin, P.D. Bilenchuk, M.S. Vertuzaev, V.B. Vekhov, A.G. Volevodz, V.O. Golubev, M.D. Dechtiarenko, E.I. Panfilova, O.G. Popov, N.A. Selivanov and some others.

It should be noted that today some special state organizations, responsible for fighting against crime in the field of high technologies, including different aspects of combating online fraud, have been established.

These types of organizations are traditionally regarded as organizations and units created by the states and included into central bodies of power: Ministries, Departments, Security Service bodies, etc.

For example, in the Russian Federation it is the Bureau of Special Technical Measures of the Ministry of Home Affairs of Russia, which includes the "K" department.

Nowadays the activity of this unit is aimed at suppression of different illegal actions. First of all it concerns crimes in the field of information technologies – such as fighting against crimes in the sphere of computer information, prevention of unlawful actions in the information and telecommunication networks, including the Internet, fighting against international crimes in the sphere of information technologies. One of the directions of the "K" department of the Bureau of Special Technical Measures of the Ministry of Home Affairs of Russia is fraud preventing measures in using electronic payment systems [1].

In the USA some special governmental organizations deal with the issues of fighting against crimes in the field of high technologies.

First of all, it is the Federal Bureau of Investigation (FBI), which included the Cyber Division created in 1996. This unit operates possessing rights of a separate body in the structure of the FBI and has four divisions, one of which deals with fighting against any kinds of fraud [2, p. 115].

In addition, the U.S. Treasury Department includes the U.S. Secret Service that investigates financial crimes in three directions:

– Crimes against the financial system (crimes against financial institutions (bank fraud), fraud with the use of electronic means of access (credit cards), money laundering);

– Crimes with the use of electronic equipment (computer fraud, fraud against telephone companies);

– Fraud against governmental financial programs (the U.S. Treasury bonds, manipulations with electronic funds transfer, other schemes) [2, p. 116].

In 2001 on the initiative of the Association of Chief Police Officers (ACPO) the National High-Tech Crime Unit (NHTCU) of the United Kingdom, Switzerland and Northern Ireland was created in the UK.

NHTCU dealt with investigating of such Internet crimes as hackings, viruses spreading, online fraud and other crimes in the sphere of high technologies connected with the use of computers and telecommunication equipment [3].

On April 1, 2006 governed by the Law "On Serious Organized Crime and Police", 2005, the National Agency for combating organized crime (Serious Organised Crime Agency – SOCA) was created having transferred the functions of departments and offices of several law enforcement agencies of the UK: of the National Crime Squad (NCS), of the National Hi-Tech Crime Unit (NHTCU), of the National Criminal Intelligence Service, of the department that deals with detection and investigation of crimes in the field of illegal use of drugs (HM Revenue & Customs – HMRC). In 2008 the Assets Recovery Agency joined the Serious Organised Crime Agency. At the same time the Serious Fraud Office remains a separate unit.

Today SOCA (similar to the Federal Bureau of Investigation of the USA) is a separate (independent organization) interdepartmental state law-enforcement agency of the UK Government, formally belonging to the Ministry of Home Affairs. It carries out its activity on the territory of the United Kingdom and cooperates (through the net of international offices) with many foreign law-enforcement and intelligence agencies [4].

It should be mentioned that since October 1, 2013 SOCA functions in regard to fighting against computer crimes have been transferred to the National Cyber Crime Unit (NCCU) of the National Crime Agency (NCA) under Article1 of the so-called "Bill of Crimes and Courts" of the UK [5].

An important role in fraud prevention in the UK is also played by a special department – the Crown Prosecution Service (CPS), namely by the Central Group of fraud prevention experts focusing their efforts on maintaining the prosecution of large and serious frauds [6].

In Germany, a special group fighting against crimes in the field of high technologies (AG EDV) was created as part of the Munich police department in 1994. Later a group "Technology" was created as part of the federal police of Germany. It includes more than 60 employees of the criminal police, technicians, engineers and scientists of different specialties. Their tasks are both independent investigation of high-tech crimes (including fraud) and promotion the work of other departments, research and development of new software and hardware for the police, international cooperation [2, p. 118].

In France, a service to combat abuses in the field of information technologies (SEFTI) was established in 1994. This unit is accountable to the Paris Criminal Police Office, and its responsibility is to fight against "intelligence" piracy and "hacking". The department of economic and financial cases of the Criminal Police (SDAEF) investigates economic crimes in the Internet. The main task of the Special Squad of Payments Fraud (BFMP) is identification of offenses connected with the use of plastic payment cards [2, p. 118].

In Canada, the responsibility to combat computer crimes belongs to the department of economic crimes (CCS) of the Royal Canadian Police. Its agencies are established in all large cities of the country (the agency includes at least one employee – an expert in a computer crime investigation). Another responsible department is the High Tech Crime Forensics Unit (HTCFU) of the Royal Police head office in Ottawa [2, p. 122].

In India, the Central Bureau of Investigation (CBI) deals with e-crimes. The Cyber Crime Research & Development Unit (CCRDU) has been functioning in its structure since 2000. The department CCRDU is engaged in collecting, storage and analyzing information on Cybercrimes [2, p. 123].

In Ukraine, a rather developed network of special units (being part of central authority bodies) has been established. It deals with combating computer crimes.

Thus, in 2001 the units to combat crime in the field of intellectual property and high technologies were set up in the structure of the State Service to Combat Economic Crimes at the Ministry of Internal Affairs. The main aim of these units is to fight against crimes in the field of computer information, electronic payments and telecommunications.

Today, after some reorganization, the Department to Combat Cybercrime has been established in the structure of the Ministry of Internal Affairs of Ukraine. It is an independent unit within the Criminal Police of the Ministry of Internal Affairs, which ensures implementation of the state policy in the sphere of combating cybercrime under the Ukrainian legislation. It organizes and carries out investigative activity within its competence and according to the law.

The main tasks of the Department, according to the Resolution regulating its activities are:

1. Participation in the development and ensuring the fulfillment of the state policy on preventing and combating criminal offences that were prepared, committed or concealed with the use of computers, systems and computer networks and telecommunication networks (in the areas of payment systems; circulation of illegal information with the use of computers, systems and computer networks and telecommunication networks (illegal content); economy which includes financial and commercial transactions conducted via telecommunication networks or computer networks, as well as prevention of economic activities prohibited in this sphere (e-commerce), the provision of telecommunications services, as well as fraud and legalization (laundering) of profits got from the above-mentioned criminal offenses.

2. Assistance in prevention, detection and termination of criminal offenses, as well as in pre-trial investigation in the way regulated by the laws of Ukraine, by the Ministry of Internal Affairs of Ukraine and by other units.

Besides the Department, some cases of fighting against cybercrimes are being handled by other divisions of the Internal Affairs bodies of Ukraine in close cooperation with other divisions of law-enforcement bodies.

For example, the responsibility of the Chief Department to Combat Organized Crime (CD COC) at the Internal Affairs Ministry of Ukraine is to organize the work in the regional subdivisions COC to combat organized criminal groups committing computer crimes, as well as informing the divisions of the Department to Combat Cybercrime about the leaders and members of organized criminal groups.

The responsibility of the criminal investigation divisions preventing offenses in this field includes implementation of measures aimed at solving crimes when, for example, electronic payment funds were the subject of the crime.

The units of the public security police must also inform the divisions of the Department to Combat Cybercrime about the individuals involved in crimes with illegal use of payment cards and other fraudulent actions on the Internet.

In addition, the structure of the Central Administration of Security Service of Ukraine includes the Department of counterintelligence protection of the state interests in the field of information security. The National Security Council of Ukraine (NSCU) includes the Interdepartmental Scientific Research Centre to fight against organized crimes. One of its main tasks is to analyze and forecast the transformation of organized crimes in Ukraine under conditions of informatization and globalization.

In this way, specialized divisions dealing with detection, investigation of computer crime, as well as gathering information on this issue at the national level have been established in many countries around the world. These are specialized national police units that are at the core of the counterforce against international computer crimes.

To the point, to ensure getting information from other countries quickly and in an available format (language of the message, specific terms, codes of the crimes, etc.) by national specialized units, as well as for a rapid exchange of such information between countries, the Interpol General Secretariat recommended all countries – members of the organization to create National Central Reference Points and to appoint special staff to work with the information on Cybercrime in 1994. Currently, these points have been created in most countries – members of the organization (usually such points are created in the Office of the National Central Bureau of Interpol or in specialized units dealing with computer crimes or economic crimes) [7, p. 211].

Taking into consideration transnational nature of computer crimes, the experience of the leading countries in gathering, research and exchange of information on the Internet fraud, computer incidents and cyber threats, can be used in other countries.

REFERENCES

1. Directions of the "K" department of the Bureau of Special Technical Measures of the Ministry of Home Affairs of Russia [Electronic resource]. – Mode of access : http://mvd.ru/mvd/structure/unit/management_k.

2. The legal and organizational principles of counteraction to crimes in the sphere of use of payment cards. Scientific and practical grant / V.M. Butuzov, V.D. Gavlovsky, K.V. Titunina, V.P. Sholomentsev; On an edition of I.V. Bondarenko. – To. : JSC publishing House of "Avanpost-Prim", 2009. – 182 p.

3. National High-Tech Crime Unit – NHTCU [Electronic resource]. – Mode of access : http://en.wikipedia.org/wiki/National_Hi-Tech_Crime_Unit.

4. Serious_Organised_Crime_Agency – SOKA [Electronic resource]. – Mode of access : http://en.wikipedia.org/wiki/Serious_Organised_Crime_Agency.

5. The Crime and Courts Bill 2012-2013 [Electronic resource]. – Mode of access : http: www.legislation.gov.uk

6. The Serious Organised Crime and Police Act 2005 [Electronic resource]. – Mode of access : http: www.legislation.gov.uk.

7. Criminalistics : the textbook / on an edition of P.D. Bilenchuk. – К. : Law, 1997 – 256 p.