DOI: https://doi.org/10.14505/jarle.7.8(22).15

Criminal Law: Combating Crimes in Financial Sphere

Mirali S. KAZIMOV
Law Department, Baku State University
Educational Centre of the Ministry of Taxes of Azerbaijan
Baku, **Republic of Azerbaijan**
vergi3m@gmail.com

Suggested Citation:

Kazimov Mirali S. (2016). Criminal Law: Combating Crimes in Financial Sphere, *Journal of Advanced Research in Law and Economics*, (Volume VII, Winter), 8(22): 2051 – 2061, DOI: 10.14505/jarle.v7.8(22).15. Available from: http://journals.aserspublishing.eu/jarle/issue/archive.

Article's History:

Received September, 2016; *Revised* October, 2016; *Accepted* November, 2016.

Abstract:

The article identifies that crime in the financial sphere as a socially dangerous act that infringes on economic and financial relations regulated by the norms of financial (tax) law, the formation, distribution, redistribution and use of funds of funds (financial resources) of States, local governments, and other business entities. It is shown that the social danger of crimes in credit-financial sphere is that as a result of such infringement is caused or created a real possibility of significant harm to the economic interests of the state, as well as other subjects related to financial activities. The authors propose to consider the criminal law not only as an institution of punishment, but also as an institution of transmission of the shadow part of the economy in the public area. This article provides analysis of the legal norms and special complex types are defined the way of development and structuring situations of counteraction to criminal law.

Keywords: legal system, criminal law, security of finance, finance enforcement, history of credit

JEL Classification: K14, K32, K40.

Introduction

Features of criminal law as an independent branch of law, determined by its own object and method. The subject of regulation of criminal law are only the social relations associated with the origin of the crime. In criminal law as the subject of the offense is the perpetrator of the crime, and the law enforcement authorities - the state.

Method of regulation of social relations criminal law is to define offences recognized by the law of crimes and punishments for committing them.

Features of criminal law is also manifested in his duties and functions. The primary duty of criminal law protection (security) of society from the most dangerous offences (crimes). Therefore, the main function of criminal law enforcement. In addition, criminal law performs the functions of General and special prevention, as well as educational.

Criminal law as branch of law, is a set of legal norms, fixed by the highest authorities in defining threat for the existing system of social relations acts as crime and punishment, and criminal responsibility and liberation from it.

When making the current new Criminal Code of the Republic of Azerbaijan were taken into account qualitative changes in recent years in political, economic and social spheres of public life of the country. In particular, it showed which of the industries protected by the criminal law, has superiority. Protection of the individual and his rights and freedoms criminal law means is in the first place. The main objects of protection of criminal law related the peace and security of mankind, the environment, state and public interests, legal rules.

Criminal law in the fight against crime is a means of implementing decisive strategic and tactical elements to crimes. At the present stage, this policy is characterized by two main trends. First, the application of severe measures of punishment against persons who have committed serious crimes or repeatedly violate the criminal law (particularly against repeat offenders, professional criminals, mafias, leaders of well-organized criminal groups). Second, limiting the scope of criminal liability for crimes that pose no great danger. So, against person who has violated the criminal law, the applicable sentence without rejection from society. This can be done conditional condemnation, to postpone execution of the sentence, and using other administrative, educational and social interventions, the replacement punishment.

1. Literature review

Worldwide the business community struggle to protect the market from unfair competition, dumping (Cheloukhine 2008, 372). With this goal established various self-regulatory organizations, which sought the right to investigate and represent the interests of an indefinite circle of entrepreneurs (Ginsburgs 1999, 321). At the same time in Azerbaijan the representatives of business communities are increasingly turning to law enforcement to protect businessmen who committed economic crimes and trying to evade criminal responsibility (Chaikin 1991, 502). Under the guise of protecting the rights of entrepreneurs pursued very different goals, in particular the termination of criminal prosecution (Naumov 1997, 221).

It should be noted that the conduct of the vast number of pre-investigation checks on crimes in the sphere of entrepreneurial activities carried out by the statements of one of the parties financial and credit relations, often using the tools of criminal repression to resolve commercial disputes (Panther 1995, 371).

In this regard, the most effective protection of the financial relations can be achieved through the implementation of measures of criminal policy aimed at the decriminalization of the economy (Gaibulloev and Younas 2016, 325). They are based should be closely coupled joint activities of law enforcement and financial control bodies (Pyne 2004, 200).

Have made the appropriate additions to the more than 20 existing regulations aimed at creating conditions for the prevention, detection and suppression of illegal financial operations, including with use of firms-'something ephemeral' and of money laundering, terrorist financing, tax evasion and customs payments, and receipt of the proceeds of corruption (Martín 2013, 337). Many of the provisions of the aforementioned Law due to the recommendations prepared by the Group of development of financial measures to combat money laundering (FATF) (Michalowski 2009, 311).

To create conditions for stable functioning and security of the financial system, prevent the harmful effects of threats of a criminal nature the need for effective state-legal mechanism of ensuring financial security, including appropriate legal and institutional components (Cartwright 2007, 18). Most of the authors consider the protection of public finances from the impact of criminal processes and abuse among the most important national interests of Azerbaijan in the financial sector (Raffaella and Masciandaro 2011, 141).

2. Counter the institutional threats of crimes in the financial sphere

The criminal law is accepted the Supreme legislative body (Milli Majlis) of the act, consisting of legal rules governing the principles and grounds of criminal responsibility, which acts are criminal, and punishment against the accused in the Commission of the persons, the conditions for exemption from liability and punishment.

Features of criminal law is that only criminal law determines criminal law: whether the act is criminal and punishable, the grounds of criminal liability, the penal system, the conditions and the procedure for their appointment and release from criminal liability and punishment and other rules. Criminal law is the single and only source of criminal law. No other legal acts or decision of the court cannot establish criminal law (Masciandaro 2008, 329).

The basis of the criminal legislation in the Republic of Azerbaijan is adopted 30 December 1999 and came into force on 1 September 2000 the criminal Code of the Azerbaijan Republic. Over the past period in the current criminal Code was introduced a number of changes. The current changes undertaken in the criminal law, held in the form of the law of the Republic of Azerbaijan on additions and changes.

The criminal Code is a systematized expression of criminal law. It consists of two parts: General and special. In the General part explains the guiding principles and General provisions of the penal law, and in a special and specific crimes, the types and limits of punishments. General and special part are in the relationship and comprise a unified whole: you cannot apply the rules of the special part without reference to the General part.

General and Special part of the Criminal Code are divided into sections or paragraphs, which, in turn, the content consists of articles (353 articles) that make up the criminal law. Articles of the General part of the Criminal Code, being rules purpose define and reinforce the principles and grounds of criminal responsibility, as well as the conditions of exemption from criminal responsibility and punishment. Unlike the General part, the norms of the Special part of the structure consists of two parts: the disposition (rule based on the signs of certain kinds of crimes) and penalties (rule based on the type and extent of punishment for a certain kind of crime).

In the General part of the Criminal Code governs the criminal law in space and in time.

The criminal law in space is based on the principles of territoriality, nationality, and reality, universality and extradition.

The essence of the principle of territoriality is that of a person who committed a crime on the territory of the Azerbaijan Republic, citizens of Azerbaijan, foreign States and persons without citizenship, are subject to criminal prosecution under the Criminal Code of the Azerbaijan Republic. However, this rule does not apply to the diplomatic representatives of foreign States and other persons, enjoys immunity, commits a crime on the territory of the Azerbaijan Republic. Thus, according to part 5 of article 11 of the Criminal Code, the question of criminal liability of diplomatic representatives of foreign States and other citizens who enjoy immunity, in case of making by these persons of a crime on the territory of the Azerbaijan Republic shall be resolved in accordance with international law.

According to the principle of citizenship of the criminal law, citizens of the Azerbaijan Republic and permanently reside in the Republic of Azerbaijan stateless persons who have committed act (action or omission) outside the Republic of Azerbaijan are subject to criminal liability under the present Code if the act is criminalized in the Republic of Azerbaijan and in the state in whose territory it was committed and if these persons were not convicted in a foreign state (article 12.1 of the Criminal Code). When the condemnation of the courts of the Republic of Azerbaijan on such persons punishment may not exceed the upper limit of the sanction provided for by the law of the foreign state on whose territory the crime was committed (Horst and Spengler 2015, 187).

In part 2 of article 12 of the Criminal Code stipulates the principle of reality. According to this principle, foreign citizens and persons without citizenship who have committed offences outside the Azerbaijan Republic may be prosecuted under the criminal law of the Republic, if the offence was directed against citizens Azerbaijan Republic, interests of the Azerbaijan Republic, and also in cases stipulated by an international Treaty of the Republic of Azerbaijan, if the criminals were not convicted in a foreign state.

The principle of universality of criminal law in space comes from the international obligations of the Azerbaijan Republic in the sphere of fight against crime. The essence of it is that regardless of a citizen of a state is a person on the territory of the state the crime was committed, any state has the power to bring him to criminal responsibility under its national law (Michelle 2004, 472).

In article 10 of the Criminal Code of the Republic of Azerbaijan enshrined in the criminal law in time. According to this article, the criminality and punishability of the acts (action or inactivity) is determined by the criminal law in force at the time of Commission of the act. No one shall be criminally responsible for an act which was not recognized as a crime at the time of its Commission. By the time of the offense shall be the time of committing a socially dangerous act (action or inaction) regardless of the time of occurrence of the consequences. In part 3 of the same article of the criminal law, eliminating criminality of an act (action or inactivity) and it is punishable, mitigates a punishment or otherwise improving position of the person who committed the crime has retroactive effect, i.e. extends on the persons who committed the act (action or inaction) prior to the entry of this law into force, and persons serving sentences or having served sentences but whose criminal record was not expunged or quashed.

Criminal law establishing the criminality of an act (action or inaction), strengthening punishment or otherwise worsening position of the person who committed the crime, is not retroactive (article 10.4 of the Criminal Code) (Levi and Maguire 2004, 462).

Amendments to the criminal code of Azerbaijan that provides for tougher penalties for committing grave and especially grave crimes, adopted on Friday at the last plenary meeting of the spring session of the Milli Majlis.

In particular, tougher penalties for terrorist acts.

Information on this issue was made by the Chairman of the parliamentary Committee on legal policy and state building of the Milli Mejlis Ali Huseynli, correspondent of Agency 'Interfax-Azerbaijan' from the hall of parliamentary sessions (Martin 2015, 63).

In accordance with the criminal code of Azerbaijan amended the terrorism (that is, the committing of explosions, fires or other actions that pose a threat of loss of life, damage their health, causing significant property damage or other socially dangerous consequences with the purpose of violating public security, sowing panic among the population or influencing decision-making by public authorities or international organizations, as well as the threat of committing such actions with the same objective) – article 214.1 of the criminal code – will be punished by deprivation of liberty for a period from 10 to 14 years. Until amendments to the criminal code, the punishment for terrorism ranged from 10 to 12 years of imprisonment.

In accordance with the criminal legislation, persons found guilty of the use of the Armed forces of the Azerbaijan Republic and other armed units stipulated by legislation of the Azerbaijan Republic, against Azerbaijan people or constitutional state organs (article 275.1 of the criminal code), will be sentenced to imprisonment for terms from 7 to 12 years, is still used of the penalty of deprivation of liberty for terms from 5 to 10 years.

For the creation is not stipulated by the legislation of armed formations or groups, which entailed death of people or other grave consequences (article 279.3 of the criminal code) will apply a penalty of imprisonment for a term of 10 to 20 years of imprisonment instead of applied to date of sanctions in the form of imprisonment from 8 till 15 years of imprisonment.

In accordance with the criminal code of Azerbaijan changes the penalties for committing the crimes under articles 100.2 (waging aggressive war), 111 (racial discrimination (apartheid)), 117.2 (announcement in fighting zones about intention to not leave anyone alive, or return his subordinates obviously criminal orders or orders directed on it, or aimed at the Commission of the crimes provided by articles 115-116 of the present Code), 275.2 (use of Armed forces of Azerbaijan Republic and other armed formations, stipulated by the legislation of the Azerbaijan Republic, against Azerbaijan people or constitutional state bodies resulting in serious consequences), 278 (violent capture of power or forcible retention of power), 280 (armed rebellion) of the criminal code, will range from 12 to 20 years of imprisonment or life imprisonment. Previously, the punishment established in the aforementioned articles of the criminal code offences included imprisonment for terms from 8 till 15 years or lifelong imprisonment.

The punishment for the planning, preparing or initiating aggressive war (article 100.1 of the criminal code) tightened with 8-10 years to 8-12 years imprisonment.

Sanctions for Commission of offences under articles 103 (genocide), 105 (destruction of the population) and 277 (an encroachment on life state or the public figure (terrorist act)) of the criminal code will now be 12 to 20 years or life imprisonment, instead of the previously used of the penalty of deprivation of liberty for terms from 10 till 15 years or lifelong imprisonment.

The punishment for committing illegal acts under articles 115.4 (murder of prisoners of war and other protected by international humanitarian law of persons), 214.2 (terrorism committed by group of persons by prior conspiracy, an organized group or criminal Association (criminal organization); repeatedly; with use of firearms and objects used as weapons; inadvertently led to the death of people or other serious consequences) and 287 (infringement of life of a person administering justice or preliminary investigation) of the criminal code that toughened the punishment of deprivation of liberty for terms from 12 to 15 years before the sanctions, which include from 14 to 20 years of imprisonment.

Sanctions for the Commission of criminal acts referred to in article 116 (violation of international humanitarian law during armed conflicts) of the criminal code increased from 7 to 15 years to 10-20 years of imprisonment.

The hijacking of an aircraft, or water transport or railway train made by organized group or entailed on imprudence death of the victim or other grave consequences (article 219.3 of the criminal code) will be punished by deprivation of liberty for terms from 10 to 15 years instead of the previously used punishment in the form of imprisonment from 8 to 15 years.

3. Methodology for the formation of stable functioning of the financial-credit sphere of the state

Providing liability for certain types of crimes in the field of computer information on the part of the legislator was the rational and correct approach, given the objective necessity, and certainly not a random character. We must not forget that the fight against crimes in the field of computer information systems in countries with existing computer system (more precisely, in countries with a high level of computerization) has become one of the main problems. There is nothing strange in the reflection of objective reality. The fact that the crimes in the sphere of computer information are socially dangerous acts and can cause considerable damage. For example, in the United States as a result of such crimes every year damages in the amount of $ 5 billion; in Germany criminals are using computers to steal every year about 4 billion Euro; in France the damage caused by crimes in the field of computer information reach 1 billion euros per year. The number of crimes in the field of computer information increasing by 30-40 % annually.

In some countries, the law, unlike the criminal code, instead of the concept of 'crimes in the sphere of computer information' the term 'computer crime'. For example, in the Netherlands adopted the Law 'On cybercrime', which uses precisely this term (Computer Crime Art). On the pages of legal literature this concept is also widespread. In scientific review, dissertation research, monographs and so on also mainly used the term 'computer crime'.

Computer crimes in the banking sector. K. P. Borishpolets provides a list of objects that are a potential target of computer crimes, in which banks are in the first place. On the other hand, we can't lose sight of that, according to experts, banking system is the most attractive sector of economy for criminals. So, they are using computer technologies to perform various socially dangerous acts in the banking sector. Data analysis of acts provides the ability to define the typical methods of committing computer crimes. First, widely prevalent computer crimes by illegal (unauthorized) access to Bank's databases through a telecommunications network. As a result of such crimes is the illegal transfer of funds in especially large size. Secondly, computer crimes are usually not committed by one person. We must not forget that such crimes in the majority are of a group nature. In other words, computer crimes in banking and computer crimes in General committed a hacking crime group (group). Hackers, being professional criminals, are the 'attackers' on the banking system. Possessing sufficient intellectual level, they are well aware of the telecommunications and computing payment technologies. On the other hand, we must not forget that they are equipped with high and advanced technical base. Hackers learn the secrets of such technical equipment and can skillfully use it. As a result, hackers have successfully 'attacked' the banks, than in his writings, the authors write in a more detailed way. Especially it should be noted that hackers hacked the computer network of commercial banks and carry out theft of funds in large volume.

Third, most computer crime in the banking sector is carried out directly with the participation of the Bank employees. Bank employees provide passwords and identity criminals. The criminals included in a computer system of the Bank, make fake payments. Then the stolen money transferred to the account in one of the banks, and using false payment orders are derived from this account.

It should be noted that computer crimes are acts that create public danger for banks. So, these acts must be considered as one of the types of crimes of a special nature committed against banking. However, for certain reasons, some authors (researchers) forget to classify computer crimes to the number of banking crimes - crimes against banking. We believe that computer crimes are criminal acts impeding the implementation of normal banking activities. Therefore, these crimes should be considered as one of the types of criminal acts against banking.

Today the concept of 'crimes in the sphere of computer information', *i.e*. 'computer crime,' stated in the criminal code, was replaced by the legislator to the concept of 'cybercrime'. In accordance with this, we should use the term 'cybercrime in the banking sector'. Chapter 30 of the criminal code called 'crimes in the sphere of computer information' and 'cybercrime'.

The reason for using the term 'cyber-crime' law makers lies in the fact that international law (documents in international law) uses the term 'cybercrime'. This, in turn, is on the International Convention 'On cybercrime' adopted by the European Council. It should be noted that a common approach to the problem of cybercrime is considered to be the main objective of the Convention. To perform this task, each state party to the Convention undertook to introduce the relevant articles of the cybercrime in the national criminal Legislation. The Republic of Azerbaijan, one of the participants of the Convention for the fulfilment of the obligation has changed the title of the Chapter of the criminal code 'crimes in the sphere of computer information' with the term 'Cybercrime'. The reason for this fact can also be explained by the fact that 'cybercrimes' are more substantial and capacious term than 'crimes in the sphere of computer information'. This generalized concept allows you to cover many types of

crimes in the sphere of computer information. Earlier, the head 03 of the criminal code provided for only two offences in the field of computer information. The researchers fairly and thoroughly indicate that these species do not cover the whole range of socially dangerous acts committed in the area of computer information. Given this situation, the legislator has completely replaced the content of Chapter 30 of the criminal code, and introduced five types of cybercrime in this Chapter. This, in turn, is about such kind of cybercrime as illegal access to computer systems for which responsibility is provided in article 271 of the criminal code.

The second type of cybercriminals – illegal acquisition of computer information, its legal regulation is carried out on the basis of article 272 of the criminal code.

The third type of cybercrime considered illegal intrusion into a computer system or computer data. The question of responsibility for the crime is classified, article 274 of the criminal code.

There is no doubt that for cybercrime under articles 271-273, criminal person uses the necessary tools (structures or computer programs). To this end, it manufactures tools and using these tools illegally intruding into a computer system (article 271 of the criminal code), computer systems or data (article 273 of the criminal code) or illegally acquiring of computer data (article 272 of the criminal code). The legislator provides responsibility for turnover (structures or computer programs) made for cybercrimes; the act is a fourth kind of cybercrime. Article 273-1 of the criminal code devoted to combating this type of cybercrime. It must be remembered that in accordance with this article, production (training) of tools for committing crimes stipulated by articles 271-273 of the criminal code, the import of such financing, purchase for use, storage, sale, distribution, or trafficking in any form entails responsibility.

Sometimes a person falsifies computer data. The goal is to give falsified computer data in authentic (authentic) data or use them. In the end, computer data specified, erased or blocked, which in turn causes violations of authenticity (authenticity) of the primary computer information. We are talking about such a socially dangerous act, as falsification of computer information, and it is the fifth form of cybercrime. Criminal law classification of this type of cybercrime is carried out under article 273-2 of the criminal code.

Thus, the existing criminal legislation provides for liability for the following five types of cybercrime:

- illegal access to a computer system (article 271 of the criminal code);
- illegal acquisition of computer information (article 272 of the criminal code);
- illegal invasion of computer systems or computer data (article 273 of the criminal code);
- the turnover made for cybercrime (article 273-1 of the criminal code);
- falsification of computer information (article 273-2 of the criminal code).

The above cybercrimes can be committed in the banking sector. We must not forget that the banking system is the main economic sector, where cybercrimes are committed. If cybercrimes are committed in the banking system, they should be covered by the concept of 'cybercrime in the banking sector'. Cybercrime in the banking sector are, of course, socially dangerous acts against banking. Thus, the analysis of individual types of cybercrime in the criminal law context, and their criminally-legal characteristic is relevant from the point of view of the study of our chosen theme, and are a matter of scientific interest.

As we noted earlier, a criminal act (cybercrime) on illegal access in a computer system that provides criminal responsibility in article 271 of the criminal code. From the criminal the right guidance it becomes clear that unauthorized entrance into a computer system or any part of, the violation of measures of protection of the system or its parts, or obtaining computer information that is stored in the system or intrusion with other personal purpose are the criminal act and provide for criminal liability.

The object of the crime are the public relations providing protection of privacy and confidentiality of computer information. Computer data shall be any information suitable for use and processing in a computer system (including facts, data, programs and concepts). Under computer system means a building or interrelated group of systems performing automatic data processing according to the programs. The information stored in the computer system, or computer data are the subject of the crime.

Socially dangerous act is an obligatory sign of the objective side of the crime of illegal access to a computer system. This characteristic, i.e. a socially dangerous act, is expressed only in the form of action. The Commission of a crime of inaction impossible.

We analyse a socially dangerous act is a crime, not with the material, and with a formal composition. So, to complete enough of the crime of illegal invasion into a computer system. From the moment of the accomplishment of this action the crime is considered complete; is not required for the effects of this illegal invasion.

As for the subjective side of the crime, it should be noted that it is characterized by direct intention. So, a person who is unlawfully intruding into a computer system or its part, is aware of the illegality and public danger

of his acts (the acts), foresaw these are socially dangerous consequences. The person also must penetrate into the computer system to retrieve stored here the computer information or other personal purpose. So, the motive is a required element of the crime.

The offender is sane person under 16 years of age. Is any person having the right of access to a computer system or part of it; the person breaches the protection of a computer system or parts of it and invades it for receiving stored data or other personal purpose. Therefore, a person under 16 years of age, becomes the subject of a crime.

If you re illegal invasion of the computer system, committing the act on preliminary arrangement by group of persons, organized group or criminal community (organization), or by abuse of their official authority, these acts are classified the relevant items of article 271.2 of the criminal code (paragraphs 271.2.1., 271.2.2. and 271.2.3). It is necessary to highlight the act of illegal invasion of computer systems in socially significant infrastructure facility or part of such system. The act provided for in article 271.3 of the criminal code. Under significant public infrastructure means public administration, enterprises, organizations, non-governmental organizations (public unions and funds), credit institutions, insurance companies, investment funds, providing important services to the state and society.

The act of illegally obtaining computer information that is one of the types of cybercrimes, classified under article 272.1 of the criminal code; criminal law context of this part it follows that the deliberate extraction of the information transmitted to the computer system from the computer system or within a system and is not subject to General use, as well as the electromagnetic irradiation of the computer systems, which are the carriers of the computer information, by technical means from unauthorised entity leads to criminal responsibility.

Before us is a kind of cybercrime is encroaching on safe storage and turnover of computer information. Therefore, the social relationships underpinning the security of computer information are the object of the crime.

As regards the objective side of the crime, it should be noted that socially dangerous act is a mandatory attribute of objective aspect of crime. The essence of the socially dangerous acts that a person gains access to computer data protected by law, without the consent and permission of the owner. We must not forget that obtaining computer information without the consent and permission of the owner is a socially dangerous act, criminal action. The offense can be committed only in the form of the action of a socially dangerous act. Obviously. Thus, the illegal extraction of computer information requires the act in the first place, the use of technology. For the form of the omission of a socially dangerous act, a crime in this form is impossible.

By design, the law, socially dangerous act is a crime with a formal composition. So, the crime is considered complete from the moment of extraction of computer information. We must remember that article 272, criminalizing the act in question does not show the consequences that determine the time of completion of the crime or its cause. If I mentioned a particular consequence, the crime would be considered completed upon the occurrence of these consequences and would have a material composition.

The subjective aspect of the crime of illegal acquisition of computer information systems is characterized by only a deliberate form. For instance, article 272.1 of the criminal code, intentional retrieval of computer information entity leads to criminal responsibility. To clarify note that the person is aware of his action, that is, the unlawfulness and danger to the public extract computer information, foresee its socially dangerous consequences. Therefore, the subjective party the crime is characterised by direct intention. The subject of criminal intent is sane person over the age of 16 before committing socially dangerous acts. Despite the lack of rights, it deliberately retrieves computer data, using technical means. Note that the legislator has determined the use of technical means as a method of committing the crime of illegal extraction of computer information. In other words, the offence must be committed by the use of technical means. Why the legislator does not define other methods of retrieving computer data? Because computer tools can be extract not only through technical means (for example, through the use of special software to unlawful use of an authentic password and code etc.). The legislator forgets about specifying these methods. We believe that the use by the legislator of the term 'various means' instead of 'technical means', it would be appropriate and would cover all kinds of funds of illicit retrieval of computer information.

In article 272.2.3 of the criminal code, envisaging responsibility for the crime of illegal extraction of computer information, we are talking about a particular subject. Under the special subject is a person abusing his official position. In the case of unlawful retrieval of computer information from officials who use their official position, his act was classified under article 272.2.3 of the criminal code.

The act on illegal access to a computer system or computer information is also considered cybercrime and the responsibility provided for in article 273 of the criminal code. According to part 1 of this article, in the case of intentional damage, destruction, damage, modification or blocking of computer information from persons without

a permit, and thereby causing damage in large amount, is subject to a separate penalty for certain criminal penalties. The object of the crime are the public relations providing safety and computer systems, and computer information. Nobody has the right to illegal access to computer information or computer system. Illegal entry is a criminal assault on the security of a computer system or computer information. Objective aspect of crime is characterized by various alternative activities listed in the provisions of article 273.1 of the criminal code and includes: deliberate damage of computer information; intentional destruction of computer information systems; intentional damage to the computer information; the deliberate modification of computer information; the deliberate blocking of computer information.

Under the deliberate damage of computer information, means the conversion of the storage medium unusable for subsequent application and use. Intentional destruction of computer information is its Erasure, in this case, it becomes impossible to use computer information. Destroyed materials also cannot be recovered. Damage of computer information means bringing information to the state when its use is properly excluded. In the case of deliberate modification of computer information, the content of computer information undergoes a transformation, losing its original form. Intentional blocking of computer information leads to temporary or permanent loss of computer information.

The presence of at least one of the alternative actions listed above, sufficient to the crime. However, these actions should result in a substantial harm. Since the causing of significant harm the crime is considered completed. So, the considered socially dangerous act is a felony with a material composition, according to the design of the legislator. The damage in the significant size implies damage in the amount of thousand manats or causing other significant damage to the interests of the state, society or individuals, protected by law, as a result of a socially dangerous act.

Damages in significant amount, can also be caused by other actions not stipulated by the legislator. For example, not taken into account by the legislator to the destruction, copying, modification of computer information, disruption of computer systems (networking) and so on. The proposed introduction by the legislator in the alternative actions that characterize the objective side of the crime.

Subjective aspect of crime is characterized by direct intention. So, if the damage, destruction, deterioration, modifications or other actions with computer information, a person aware of the illegality and social danger of his actions, he foresees his danger to the public and wants it.

The offender is sane person over the age of 16 before committing socially dangerous acts. In other words, a sane person over the age of 16, is subject to criminal liability for the act, and the person recognized by the offender.

Article 273.2 of the criminal code criminalizes the intentional serious hindering the activities of the computer system, and the act is considered a form of illegal invasion into a computer system. According to this article, the intentional perpetration of serious obstacles to the activities of a computer system by inputting, transmitting, damaging, erasing, damaging, modification or blocking of computer information from the person who does not have permission to do so, leads to responsibility.

The object of the crime are the public relations providing normal functioning of a computer system. It is obvious, since the criminal intent of encroaching on the public relations providing normal operation of the computer system.

There is no doubt that the obstruction of the activities of the computer system can be committed through alternative actions such as entering, transferring, damaging, erasing, defacing, modification or blocking of computer information. It is for this reason, the objective aspect of crime is characterized by the above alternative actions, the Commission of one of them leads to serious disturbances in the functioning of a computer system. Serious obstruction of the activities of the computer system involves such a violation, which restricts the possibility of using this system or exchange data with other computer systems on the part of the owner or user of the computer system.

Subjective aspect of crime is characterized by direct intent; the subject is considered to be a sane individual over the age of 16 before committing a socially dangerous crime.

We now turn to the criminal legal characteristic of the other cybercrimes. We are talking about the analysis of criminal acts, under article 273-1 of the criminal code, in the criminal law context. According to part 1 of this article, the main purpose of its preparation or adaptation is bringing to responsibility for the production of structures or computer programs, which are tools for committing crimes provided for in articles 271-273 of this Code (article 271 of the criminal code - illegal access to a computer system; article 272 of the criminal code - illegal removal of the computer information; illegal intrusion into a computer system or computer data - article 273 of the criminal code), as well as the import, acquisition for the purpose of using, storing, selling, distributing, or

facilitating the acquisition of other ways such structures or computer programs, with the aim of committing the same crime entailing damage to a significant amount of. It should be noted that this type of crime has a material composition, that is, a socially dangerous act with the material composition. So, to complete the crime requires a damage in large amount, and since its application, the crime is completed.

RNAi information, we are talking about a particular subject. Under the special subject is a person abusing his official position. In the case of unlawful retrieval of computer information from officials who use their official position, his act was classified under article 272.2.3 of the criminal code.

The offence in question has two objects: the main object of the crime is considered to be social relations that ensure the prevention of cybercrime; as additional object of accepted social relations, preventing a turnover, made for cybercrime.

Objective aspect of crime is characterized by several alternative activities listed in the provisions of article 273-1.1 (production, import, purchase with intent of use, possession, selling, distributing and facilitating the acquisition of other ways structures or computer programs to commit these crimes). The Commission of one of the alternative actions enough to commit the crime.

Subjective aspect of crime is characterized by direct intent; the subject is considered to be a sane individual over the age of 16 before committing a socially dangerous crime.

We have provided criminal legal characteristics of the five types of cybercrimes stipulated in the existing penal legislation of AR, found them (the elements). However, these types of cybercrimes do not reflect all socially dangerous acts committed in the field of information technology (computer information). In other words, the criminal code does not reflect all the types of cybercrime. The fact is that Chapter 30 of the criminal code does not specify liability for certain types of cybercrime. We believe that the legislator should consider the inclusion of articles establishing liability for some types of cybercrime, previously not provided for in the criminal code.

This, in turn, is the formulation of a legislator separate article providing responsibility for theft of funds by means of computer technology. The act is one of the types of cybercrime. You need to consider that at the present time widespread criminal act the theft of money, through the use of computer tools. It is no secret that as the main object of the crime, the attackers choose the banks. By entering a false (not true) the data in the commercial system of the Bank, the criminals carry out theft of funds in large sizes. Most of these crimes are committed directly by employees of the Bank. Criminals are part of the Bank's computer with a modem and using the password and identification data (in some cases provided by the banking workers), carry out fraudulent payments. Then the stolen funds are transferred to an account at another Bank. Then by payment order or in other ways the scammers to withdraw money from the account.

We should also consider theft of Bank funds through the use of computer equipment by hackers. Hackers 'running and acting' in a separate guarded building, carry out theft of funds in large amount of illegally intruding into a computer system of the commercial banks, through advanced technology.

For a legal assessment of acts of theft of funds using computer technology it should be noted that usually the theft is classified as secret theft of property of a third party (article 177 of the criminal code). Law enforcement agencies in certain cases, depending on the implications of criminal activities (fraud), classify such acts as embezzlement through abuse of trust or deception, *i.e.*, fraud (article 178 of the criminal code). This approach to the question no more than the application of criminal law by analogy.

The criminal code also prohibits the application of law by analogy. In article 5.2 of the criminal code it is noted that you cannot apply the law by analogy. The question arises: by what right do the theft of money using computer technologies is categorized as theft (article 177 of the criminal code) or fraud (article 178 of the criminal code). Isn't that a violation of such important provisions of the criminal code as 'not permitted application of the criminal law by analogy.'

The best option that the legislator should introduce a separate article providing responsibility for theft of funds through computer technology. This proposal is reasonable and defensible from the criminal law point of view. Our proposal is to recognize theft of funds with the use of computer means independent of the criminal structure. It must be remembered that there is a similar article in the criminal code of some countries. For example, the criminal code of the Republic of Belarus exactly resolves this problem: according to art. 212 of the criminal code provides for liability for theft of property by modifying the information used in a computer system, stored on machine-readable media or transmitted via information transmission networks. It is necessary to consider that the Model Criminal code for the countries - participants of the CIS proposed the introduction of an independent criminal motives against theft using computer technology, in national criminal law.

Undoubtedly, modification of computer information of a third party is a public dangerous act committed by deception or abuse of trust, and leads to the infliction of damage to property. We believe that the legislator should

recognize the act as an act with criminal composition, and make a separate article in the criminal code, providing responsibility for the act.

I would like to raise another issue: sometimes the person carries out the illegal access to computer system of a third party, for the purpose of extracting data contained in the system, or without other personal purposes (in the case of such objectives, the classification of the acts is carried out according to article 271 of the criminal code).

For example, illegal access to computer system aims at familiarization with the data stored in the system, that is not the reason causing any damage. We are talking about the introduction to information system of a third party by unauthorized access without damage (in contrast to illegal entry into the apartment of a third party). The criminal code does not envisage liability for such an act. The question arises: why the current legislation does not accept this act as a crime, and the illegal penetration into the apartment believes a criminal act? We believe that it would be appropriate if the legislator will pay due attention to the preparation of the answer to this question. We must not forget that as the apartment is, the information system of the third person are inviolable. Therefore, without the permission of the owner, no one has the right to encroach neither on someone else's property or in the information system. As well as the property information system should be protected by criminal law means.

Conclusion

In conclusion, it should be noted that the country's economic and financial situation is greatly complicated by the substantial criminalization of the budget and the banking sector, organized criminal activity within credit and financial organizations and institutions, microfinance organizations, as well as the creation of 'financial pyramids' harmful to Federal public authorities, public corporations and companies, all types of businesses and hundreds of thousands of citizens of the Azerbaijan.

All this indicates the need for a systematic orientation of law enforcement agencies on combating banking crime. We cannot exclude the establishment of special state law enforcement body, endowed with special competence in the field of financial-credit relations. In addition, it appears that the issues of ensuring financial security needs to find some reflection in national security Strategy of the Azerbaijan, and the state's criminal policy should be aimed at achieving the goals of this Strategy.

Currently, law enforcement and judicial authorities effectively used the mechanisms of criminal policy of the state. However, it is not enough to solve the issues of financial security of the state only criminal methods, it is necessary to expand the set of measures in the context of the Government of the Azerbaijan of a uniform financial, credit and monetary policy.

References

[1] Barone, Raffaella, and Donato, Masciandaro. 2011. Organized crime, money laundering and legal economy: theory and simulations. *European Journal of Law and Economics* 32(1):115-142. DOI: 10.1007/s10657-010-9203-x.

[2] Chaikin, David, A. 1991. Money laundering: An investigatory perspective. *Criminal Law Forum* 2(3): 467-510. DOI: 10.1007/bf01096484.

[3] Cheloukhine, Serguei. 2008. The roots of Azerbaijann organized crime: from old-fashioned professionals to the organized criminal groups of today. Crime. *Law and Social Change* 50(4): 353-374. DOI: 10.1007/s10611-008-9117-5.

[4] Cartwright, Peter. 2007. Crime, punishment, and consumer protection. *Journal of Consumer Policy* 30(1):1-20. DOI: 10.1007/s10603-006-9026-x.

[5] De Sanctis, Fausto, Martin. 2015. Criminal Investigations and Cases Involving Financial Crimes Practiced by and Through Religious Institutions. *In Churches, Temples, and Financial Crimes: A Judicial Perspective of the Abuse of Faith*, 45-87. Cham: Springer International Publishing. DOI: 10.1007/978-3-319-15681-1. ISBN 978-3-319-15681-1,

[6] Entorf, Horst, and Hannes, Spengler. 2015. Crime, prosecutors, and the certainty of conviction. *European Journal of Law and Economics* 39(1): 167-201. DOI: 10.1007/s10657-012-9380-x.

[7] Gaibulloev, Khusrav, and Javed, Younas. 2016. Conflicts and domestic bank lending. *Public Choice* 169(3): 315-331. DOI: 10.1007/s11127-016-0362-3.

[8] Gallant, M., Michelle. 2004. Assaulting the Financial Underpinnings of Crime. *Criminal Law Forum* 15(4): 471-475. DOI: 10.1007/s10609-005-2993-9.

[9] Ginsburgs, George. 1999. Extradition of Fugitive Criminals under the CIS Convention on Legal Assistance in Azerbaijan's Law and Practice. *Criminal Law Forum* 10(3): 317-357. DOI: 10.1023/a:1009440717619.

[10] Levi, Michael, and Mike, Maguire. 2004. Reducing and preventing organized crime: An evidence-based critique. *Crime, Law and Social Change* 41(5): 397-469. DOI: 10.1023/B:CRIS.0000039600.88691.af.

[11] Martín, Ana, M., Bernardo, Hernández, Stephany, Hess, Cristina, Ruiz, and Isabel, Alonso. 2013. The Relationship Between Moral Judgments and Causal Explanations of Everyday Environmental Crimes. *Social Justice Research* 26(3): 320-342. DOI: 10.1007/s11211-013-0188-9.

[12] Masciandaro, Donato. 2008. Offshore financial centres: the political economy of regulation. *European Journal of Law and Economics* 26(3): 307-340. DOI: 10.1007/s10657-008-9075-5.

[13] Michalowski, Raymond. 2009. Power, crime and criminology in the new imperial age. *Crime, Law and Social Change* 51(3): 303-325. DOI: 10.1007/s10611-008-9163-z.

[14] Naumov, Anatolyi, V. 1997. The New Azerbaijann criminal code as a reflection of ongoing reforms. *Criminal Law Forum* 8(2): 191-230. DOI: 10.1007/bf02677783.

[15] Panther, Stephan, M. 1995. The economics of crime and criminal law: An antithesis to sociological theories? *European Journal of Law and Economics* 2(4): 365-378. DOI: 10.1007/bf01541074.

[16] Pyne, Derek. 2004. Can Making It Harder to Convict Criminals Ever Reduce Crime?. *European Journal of Law and Economics* 18(2): 191-201. DOI: 10.1023/B:EJLE.0000045081.01565.ed.

***Criminal Procedure Code of 14 July 2000. Available at: http://www.legislationline.org Unofficial English Translation. Adoption: 2000-07-14 | AZE-2000-L-64892

***Criminal Code of 30 December 1999. Adoption: 1999-10-30 | AZE-1999-L-64893

***Law No. 194 of 9 October 1999 on additional measures in relation with the realization of legal reforms in the Republic of Azerbaijan, the improvement of the work of judges, corrective labour establishments and confinement. Adoption: 1999-10-09 | Date of entry into force: 1999-10-09 | AZE-1999-L-64882

***Law of 5 October 1999 to amend several legal acts. Adoption: 1999-10-05 | AZE-1999-L-64878.