International crime as a threat to global socio-economic security

Serik M. Apenov*

Department of International Law,
Al-Farabi Kazakh National University,
Almaty, Republic of Kazakhstan

*Corresponding author

Nurbol S. Jetibayev

Department of Law,
Narxoz University,
Almaty, Republic of Kazakhstan

Mariyash K. Makisheva

Department of Diplomatic Translation,
Al-Farabi Kazakh National University,
Almaty, Republic of Kazakhstan

Guldana A. Kuanalieva

Department of Customs, Financial and Environmental Law,
Al-Farabi Kazakh National University,
Almaty, Republic of Kazakhstan

Sergazy Kussainov

Department of Criminal Law Disciplines,
Abai Kazakh National Pedagogical University,
Almaty, Republic of Kazakhstan

Abstract: The authors identify the concepts of international and transnational crime, focusing on its innovative component – the absence of the need for contacts and decentralisation of the sources of the criminal community. In particular, virtual organised criminal communities are analysed. The novelty of the research lies not only in their historical analysis, but also in the formation of a mechanism to counter them on the basis of a structural and international legal approach. The already implemented countermeasures are analysed and the international legislative acts that constitute the mechanism of global cyber

security are structured. The practical significance of the study is determined by the fact that the developed comprehensive analysis of the phenomenon can be applied to the strategies of the socio-economic development of the state in the section of possible risks and compensation for losses from their implementation.

Keywords: international crime; organised crime; property; cyber security; legal measures.

Reference to this paper should be made as follows: Apenov, S.M., Jetibayev, N.S., Makisheva, M.K., Kuanalieva, G.A. and Kussainov, S. (2021) 'International crime as a threat to global socio-economic security', *Int. J. Electronic Security and Digital Forensics*, Vol. 13, No. 2, pp.133–154.

Biographical notes: Serik M. Apenov received his PhD in Law, and an Associate Professor of the Department of International Law, Al-Farabi Kazakh National University. In 2004, he defended his PhD thesis on the theme 'Forms of complicity under the legislation of the Republic of Kazakhstan (issues of theory and practice)'. He has more than 50 scientific publications, including one monograph, one textbook, three books, articles, and other publications.

Nurbol S. Jetibayev received his PhD in Law, and an Associate Professor of the Department of Law at Narxoz University. In 2009, he defended his PhD thesis on the topic 'Improper performance of medical staff in their professional duties'. He has more than 50 scientific publications, including one monograph, one textbook, articles, and other publications.

Mariyash K. Makisheva is an Associate Professor of the Department of Diplomatic Translation in Al-Farabi Kazakh National University. She has more than 80 scientific publications, including five textbooks, articles and other publications. She is a developer of consecutive and simultaneous translation. She was awarded by the Ministry of Education and Science for her significant contribution to the educational process and for the achievements and high level of language teaching in the specialty. She participated at the 13th European Conference on Management, Leadership, and Management in London (UK).

Guldana A. Kuanalieva is a Full Doctor in Law, and a Professor of the Department of Customs, Financial and Environmental Law at Al-Farabi Kazakh National University. In 2003, she defended PhD thesis on the topic 'Causal relationship in criminal law'. In 2010, she defended her doctoral thesis on the topic 'Problems of personal security in criminal proceedings of the Republic of Kazakhstan'. She has more than 80 scientific publications, including two monographs, one textbook, articles, and other publications.

Sergazy Kussainov received his PhD in Law, and an Associate Professor. In 2012, he defended his PhD thesis on the topic 'Formation and development of forensic science in Kazakhstan'. He has more than 30 scientific publications, including one monograph, one textbook, articles, and other publications. He participated at the International Congress of scientists in Bishkek (Kyrgyzstan).

1 Introduction

Each person has the right to own, use and dispose of his property, the results of intellectual and creative activity. In turn, the duty of the state is to ensure their protection and implementation, since one of the functions of the state is to protect the interests of citizens from external and internal hazards. Recently, the dependence of mankind on new technologies is growing at an incredible rate. However, this progressive trend, unfortunately, carries with its negative consequences.

The rapid introduction of new technologies in the fields of electronics, communication and digital technologies in the late 20th and early 21st centuries led to the emergence of new public relations and related problems associated with the human desire for development, ease of work and improved living conditions (Bergeron, 2013). The greatest importance in this process was acquired by the internet technology, which provided virtually unlimited possibilities in transmitting, distributing and receiving information, communication, performing a number of actions, regardless of the time and place of stay of the person. At the same time, the discovery of new horizons for the world community is inextricably linked with the emergence of new forms of criminal activity and other manifestations of the unfair use of the achievements of scientific and technological progress (Zysset, 2018).

The need to improve the foundations of the legal regulation of the fight against cybercrime is one of the priorities, therefore, the relevant legal regulations must meet the requirements of the times and modern conditions (Kryvoi, 2018). Accordingly, each stage of the formation of this institution, both in the world and in the Republic of Kazakhstan, significantly affected the legal regulation of activities on the internet and the protection of the interests of citizens from cyber threats (Leonov and Ayaganova, 2018; Zhuravel and Kurumisawa, 2019). That is why the study of the formation of legal regulation of the fight against cybercrime in the Republic of Kazakhstan and the world is relevant, since it will establish at what level of development this process is in our state today and relate to similar global processes. In addition, building a successful and effective mechanism for the legal regulation of the fight against cybercrime is impossible without paying due attention to the historical prerequisites for its emergence and development.

The Republic of Kazakhstan is at the initial stage of the fight against computer crimes, but a targeted policy on the legal regulation of the fight against cybercrime is still being implemented. Therefore, it is important to analyse this relatively short way of the national legislator to solve existing problems with the emergence and spread of new forms of crime and to establish a relationship with the history of the development of this phenomenon at the global level.

The rapid development of scientific and technological progress led to the use of electronic computing machines (computers), computer networks and various electronic communication systems in almost all spheres of public life. At the same time, as a result of the proliferation of the above-mentioned technical innovations, negative social phenomena have arisen related to the activities of the corresponding equipment and technology, in particular information crimes. Under these conditions, the Republic of Kazakhstan has an urgent need to ensure the effective fight against cybercrime, which, among other things, includes the mechanism of legal regulation of relevant public relations.

The growing number of informational crimes, the severity of the consequences caused by them, the cross-border nature and other negative factors necessitate the introduction of close international cooperation in this industry, which presupposes the effective functioning of both national and international measures to combat cybercrime. Therefore, an extremely relevant theoretical and practical issues is the issue of the structure of the mechanism of legal regulation of the fight against cybercrime and its international legal regulation. The study of the subject matter allows us to find out the existing system of normative regulation of public relations in the field of countering information crimes, identify gaps and weaknesses of the existing regulatory framework, identify priority areas for improving regulatory regulations, as well as prospects for international legal cooperation.

Therefore, it is necessary to carry out a doctrinal analysis of the current state of the structure of the mechanism of legal regulation of the fight against cybercrime and its constituent elements. Special attention should be paid to the problem of international cooperation: interaction of law enforcement agencies of various states, borrowing joint experience, conducting special exercises, promptly exchanging the necessary information, etc., that is, appropriate international legal regulation of the fight against cybercrime.

2 Literature review

In the scientific legal literature, it is noted that the concept of 'mechanism of legal regulation' was developed and introduced into the doctrine of law in the years of the rule of Soviet law (Allum and Sands, 2004). As for the legal regulation mechanism itself, this category was scientifically substantiated in sufficient detail in the definition and provision of the characteristics of the constituent elements, as well as in the definition of significance for legal science and law in general. At the same time, the further development of scientific thought in the direction under study was not limited to the achievements of legal scholars of the Soviet period. So today, in the scientific legal literature, both on the problems of the theory of law and within the sectoral legal disciplines, other concepts of understanding the investigated legal phenomenon have been proposed and doctrinally substantiated.

They propose to consider the 'legal regulation mechanism' as taken as a whole, the totality of legal means by which legal influence on public relations is ensured (Calderoni, 2011). That is, the category under investigation is determined by a certain list of legal tools that influence social relations, which allows them to regulate in a normative way. This position is considered to be a classic in legal science and has a number of positive aspects, however, it is also not without some flaws. For example, from the analysis of the author it is not clear for what purpose the normative influence is exercised, what is necessary to be understood by the term legal means and the like.

Additionally, a legal regulation mechanism is defined as a system of legal means organised in the most consistent way (Schroeder and Friesendorf, 2009). At the same time, with such an approach it is difficult to understand why the organisation of the corresponding legal means is carried out, how they are influenced, which creates the most consistent organisation and so on. We believe that this approach is extremely simplified and does not allow to fully disclose the essence of the concept under study.

The mechanism of legal regulation is proposed to define as a set of legal means by which the behaviour of the subjects of public relations is brought into compliance with the requirements and permissions contained in the law (Williams and Godson, 2002). That is, the legislator establishes the legislator certain permissions and prohibitions that are binding on the subjects of legal relations, which allows regulating their desired behaviour in public life. This approach seems to be more logical and consistent, since regulatory prescriptions do not affect the relations themselves, which arise, change, and cease in society, but the corresponding subject circle of people, their behaviour, which predetermines the transformation of legal relations.

The mechanism of legal regulation is a system of legal means by which orderliness of social relations is carried out in accordance with the goals and objectives of the rule of law. From the analysis of the above doctrinal definition, one can establish the characteristic features:

1 is a system of legal means

2 ensures the orderliness of relations that arise, change and cease in society

3 meets the goals and objectives of the rule of law.

The category under investigation is defined as a system of legal means, methods and forms by which the normativity of law is transferred into the orderliness of social relations that satisfies the interests of legal entities, and the rule of law is established and maintained. Thus, the scope of legal tools, which helps to ensure the regulatory impact of the law on public relations, is significantly expanded, namely: along with legal means, legal forms and legal methods are proposed. Such an approach seems doubtful in view of what is meant by the appropriate forms and methods, that is, whether they are able to provide normative influence on relations existing in public life and how they relate to the concept of 'legal means'.

In addition, they propose the following definition of a 'legal regulation mechanism' this is an abstract general legal regulation mechanism that is applied specifically and particularly to a concretely-defined case (and form) of the legal force of the law in force (von Lampe, 2006). The definition differs significantly from the rights in the doctrine of law, since it defines the legal category under investigation in a different way, because its key features are:

1 in essence, it is an abstract mechanism of legal influence

2 is individually expressed to the specific case of application of the legal prescription.

Under such conditions, the position seems to be wrong, when speaking about the mechanism of legal regulation, they imply a clear and effective system of legal tools that provides a normative influence on the behaviour of an unspecified number of subjects of public relations in all such cases when such a rule should be applied.

In the scientific legal literature it is indicated that the pluralism of opinions on the studied legal concept allows defining such approaches of understanding the legal nature of the category 'legal regulation mechanism': instrumental; activity; comprehensive; integrated. Each of the above doctrinal concepts has both its supporters and opponents, who point to the 'strong' and 'weak' sides of these theoretical positions. Under such conditions, none of them is correct and exhaustive, therefore, to study the problems of the

structure of the legal regulation of the fight against cybercrime, it is advisable to analyse them and identify rational aspects (Van Dijk, 2007).

Thus, the 'legal regulation mechanism' as a law category is aimed at streamlining the phenomena of legal reality, ensuring their unity, interconnection and interaction, which is expressed in the possibility of transforming legal norms into real influence on the behaviour of subjects of public legal relations. The concept of 'legal regulation mechanism' can generally be defined as a clearly established and organised system of legal tools that ensures the law impact of regulatory prescriptions in the sphere of public relations, which allows regulating the limits of permitted and prohibited behaviour of participants in the relevant circle of public relations in order to ensure law and order in accordance with the needs and interests of the state, civil society, individuals and the like (Boylan, 1997).

In sectoral legal sciences there are also available doctrinal works of legal scholars regarding the understanding of the relevant mechanism within a particular branch of law or legal science. Studying the issue of the 'mechanism of criminal procedure regulation' we emphasise that it is the system of procedural means provided for by the structure of criminal procedural law, with the help of which the regulation of social relations arising in the field of criminal justice is ensured. A comprehensive means of such regulation is criminal procedural law, the purpose of which is to effectively regulate these relations. A feature of this approach is that it should be defined as a means of legal regulation of an independent branch of law – criminal procedural law, which provides a comprehensive regulatory impact on the entire sphere of criminal procedural relations, including the behaviour of participants in such legal relationship. At the same time, it is impossible to fully agree with these arguments, since the branch of law, first of all, is a set of legal norms, and the category 'legal regulation mechanism' in its structure is not limited to normative prescriptions, but includes other legal phenomena in its scope.

Analysing the corresponding definition, it can be concluded that it is based on an instrumental approach, which defines the category under investigation as a set of legal tools (means, forms, methods, principles, relationships, connections between them), which provide an opportunity to influence criminological objects to complete the tasks (Levi and Maguire, 2004). Taking into account the above, the category 'mechanism for legal regulation of the fight against cybercrime' can be defined as a well-defined and organised system of legal tools that provides law impact through the application of regulations on social relations that arise, change and end in the field of countering the commission of information crimes, that allows you to influence the desired behaviour of participants in such relationships, with the aim of achieving appropriate and effective fight against cybercrime.

Discussion in terms of understanding the legal nature and essence of the concept under study, gives rise to numerous doctrinal concepts regarding the understanding of the structure (internal structure) of this legal phenomenon (United Nations Centre for International Crime Prevention, 2000). One of the most voluminous and cumbersome approaches is the so-called 'wide', which provides that the legal regulation mechanism includes such constituent elements as: the rule of law, the direct regulator of the behaviour of subjects of law, gives them a certain amount of mutual subjective rights and legal obligations; regulatory legal act; legal fact; legal relations; the interpretation of law; realisation of law; legality, the implementation of legal regulations through compliance with legal requirements by legal entities; legal awareness, the awareness of the subjects of legal regulations; legal culture; lawful behaviour; illegal behaviour; legal liability.

However, with this approach, some of the above constituent elements can hardly be attributed to the structure of the studied legal category (for example, legal consciousness, legal culture, and some others). It is also doubtful that a significant amount of legal means can belong to the internal structure of the category being studied (Beken, 2004). Diametrically opposed to the above concept is the so-called 'narrow' understanding of the structure of the mechanism of legal regulation, which implies the presence of such constituent units: the rule of law; regulatory legal acts; legal relations; realisation of law; legality.

Each of the elements of this system performs a specific function of satisfying the interests of subjects, in regulating social relations, in achieving the effectiveness of legal regulation. This approach also does not seem ideal, since it is difficult to understand why it is necessary to single out the norms of law and regulations, where the regulatory prescriptions are contained in separate constituent elements (Edwards, 2001). In addition, the expediency of attributing legality to the composition of the structure of the mechanism of legal regulation is questionable, because it is more correct to define the rule of law, which is a broader and more general concept. Thus, the concept of 'narrow' is also quite controversial and poorly argued from a doctrinal point of view.

It is necessary to highlight such basic elements of the mechanism of legal regulation as: regulatory framework; legal relations; the implementation of the subjects of their rights and obligations. Regarding the last of these elements, we believe that the choice is erroneous, because it mediates the realisation of the behaviour of participants in the relevant social relations, that is, it's about the actual content of legal relations, which is already an integral element of the category being studied, and therefore its separate aspect singled out as an independent structural element (Shelley and Picarelli, 2005).

The structure of this mechanism includes the following elements:

1 the rule of law and its principles, expressed in legal acts, presidential decrees and other regulatory acts

2 acts of interpretation of legal norms issued by authorised organisations

3 acts of application of the law

4 legal relations.

Analysing the proposed approach, it should be noted that the need to define acts for the implementation of legal norms is unclear, since in this case we are also talking about the implementation of legal behaviour by the subjects, that is, again it is about the legal relations that are independent constituent elements. There are also doubts about the definition of the need for acts of interpretation of the law as elements of the structure of the mechanism of legal regulation, since there are a significant number of types of interpretation and it is not clear which of them are involved in such cases. We propose the identification of three main elements in the mechanism of legal regulation:

1 legal norms

2 legal relations

3 acts of realisation of rights and obligations; and an optional element – acts of law.

A similar position was expressed by Soviet researchers, who called the three main and several auxiliary elements of the mechanism of legal regulation. They referred to the

main ones (Tripp and McMahon-Howard, 2016): legal norms; legal relations; the implementation by participants of legal relations of their subjective rights and obligations. Auxiliary they called the acts of application of the law, and the regulatory basis of the named mechanism – the system of legal norms. However, the behaviour of subjects of public relations is regulated by determining the type of regulations and the measures according to which they are forced to build their behaviour (Blum, 1997). That is, it is about the fact that acts of real behaviour are the actual content of legal relations, and under such conditions legal relations are the means of the mechanism of legal regulation, the acts of realisation of the law constitute their content.

In general, separating the existing approaches in the theory of law to the definition of legal means of a legal regulation mechanism, it can be argued that each element of such a mechanism has a specific role in regulating people's behaviour and social relations arising on this basis (Hagan, 2006). Therefore, we believe that the following elements are included in the structure of the mechanism of legal regulation of the fight against cybercrime: law rules; legal relations; legal facts (Kramer, 2016; Finckenauer and Chin, 2006). Thus, ensuring an effective fight against cybercrime at the present stage of social development requires appropriate international regulatory framework, so it is advisable to examine the current state of the relevant legal framework and identify key areas for improvement.

3 Materials and methods

This issue is new to the legal doctrine of our state, since by this time a comprehensive study of the genesis of domestic and international legislation on combating cybercrime has not yet been carried out. At the same time, a lot of work has been devoted to the issue of cybersecurity, cybercrime and their legal regulation. However, the issue of the genesis of the legal regulation of the fight against cybercrime in the world and the Republic of Kazakhstan was not considered as a whole, the stages of development of this phenomenon were not highlighted.

Advent of cybercrime is associated with the spread of the so-called virtual space, which contains information about individuals, events, phenomena, processes, etc., encrypted in mathematical, symbolic, or any other form. Therefore, it is clear that cybercrime is a relatively new type of criminal activity, which requires special skills and knowledge and the specificity of which lies in the fact that the technical capabilities for its commission appeared relatively recently, and therefore it is worth referring to the historical prerequisites for its appearance and development.

Advent of the term 'computer crime' is chronologically associated with the beginning of the 60s of the last century, when the first cases of crimes committed with the use of electronic computers were identified. The USA is considered the 'homeland' of this type of crime, where in 1945 the first electronic computer was created, one of the earliest forms of computers that was used to decipher German military codes, and later with a different purpose. The same thing happens in our time, when computers and network systems are used primarily for solving information security problems, and only then for other local purposes. Therefore, it is not by chance that the commission of the first in the history of computer crime occurred in Minnesota, where in 1966 the first case of using an electronic computer as a tool was recorded during a bank robbery. Subsequently, the emergence and spread of computer equipment and advanced technologies appeared as a

real threat to the national security of states. Scientists have begun to worry about this issue, for example, since 1958, legal statistics from the Stanford Research Institute characterise the types of 'computer' crimes of the 20th century:

1 cases of damage and theft of computer equipment, theft of information

2 fraud or theft committed with the use of computers

3 unauthorised use of computers or theft of computer time.

That is, at that time a clear understanding of the emergence of a new type of crime and the need to overcome it was already formed at the scientific level. Despite the prompt reaction of scientists, everything indicates that the states of the world were not ready for the emergence of such threats.

At the moment, there is no evidence of the existence in those days of appropriate legal instruments to combat cybercrime, nor of punishing those responsible for committing criminal acts related to computer and network activities. Note that at that time, computer crime was finally formed as an independent element of the criminal system, since the 1970s are characterised by the appearance of the first professional computer criminals – hackers. It is worth noting that one of the first hackers was Steve Wozniak and Steve Jobs, who started the production of devices for hacking telephone networks. So, the period from the beginning of the 60s of the 20th century to the beginning of the 70s should be considered the first, preparatory, stage of development of cybercrime. His dating was chosen taking into account the fact that the initial moment should be considered the first cases of crimes committed with the use of electronic computers. Accordingly, at the end of this stage, computer intruders were already organised criminal groups, who used their knowledge for illegal enrichment and violation of the established order.

So, for the first, initial stage of development, the following features are characteristic:

1 the first cases of crimes committed with the use of electronic computers

2 the formation of organised criminal groups that used their knowledge for illegal enrichment and violation of the established procedure

3 the lack of legal instruments to combat cybercrime

4 the absence of cases of punishment of computer criminals for their illegal activities.

It should be noted that at the scientific level, the understanding of the danger of the spread of cybercrime has been further developed and subsequently systematised into separate provisions and concepts. For example, the American Bar Association in Dallas in 1979 for the first time formulated the main features of computer crimes:

1 use or attempt to use a computer, computer system or network of computers in order to receive money, property or services under the guise of false pretenses or false promises, or posing as another person

2 intentional unauthorised action aimed at changing, damaging, destroying or stealing a computer, computer system, network of computers or computers that have software systems, programs or information

3 deliberate unauthorised disruption of communication between computers, computing systems or networks of computers.

At that time, the phenomenon of cybercrime had already spread to the territory of the former USSR, which also included the Republic of Kazakhstan – in 1979 in Vilnius; as a result of cybercrime, the state was damaged in the amount of 80 thousand rubles. That is, the difference in the development of computer crime in the world states and in the Soviet Union was about two decades, which is clear evidence of how significant there was and there is a difference in the development of legal tools to combat cybercrime. If at this stage certain bases of legislation on cybercrime already functioned on the territory of more developed states, for the USSR computer crimes appeared as a completely new phenomenon.

At that time, cybercrime had already spread significantly around the world, and the fight against it had become global. In 1983, a historic event took place in the USA – the first arrest of a cybercriminal, about which the public became aware. A group of teenagers carried out online hacking about 60 computers. After the arrest, one of the participants testified, so that all other members of the organised group received a suspended sentence. This moment is important in the context of our research at once for a number of reasons:

1 arrest and punishment is evidence that at that time there were already legal norms that contained signs of legislation on cybercrime

2 a suspended sentence for criminals demonstrates that this type of crime was not considered as having a high level of public danger

3 cybercrime and cybercriminals began to be reported to the public, that is, the fight against cybercrime was only gaining momentum.

The next significant event that is directly related to the genesis of legal regulation of the fight against cybercrime in the world took place in 1986, when the USA adopted the first ever computer law 'The Computer Fraud and Abuse Act' (United States Code, 2017), which prohibited unauthorised access to computer systems and obtaining secret military information. In addition, the law defines and protects three types of unclassified information:

- information belonging to financial institutions, such as credit card and account information
- data from government agencies
- information belonging to international or interstate organisations.

Important consequences of the entry into force of this legal act are:

1 it was forbidden to spread viruses, which at that time were widespread

2 in 1986, the hacker was first arrested – Lloyd Blankenship.

Thus, the moment of adoption of the first in the history of the regulatory legal act on cybercrime is associated with the completion of the second stage of development.

The spread of cybercrime (the beginning of the 70s of the 20th century – 1986) is characterised by the presence of the following main features:

1 a clear formation of the concept of computer crimes at the scientific level

2 the spread of cybercrime into the territory of the Soviet Union, which also included the Republic of Kazakhstan

3 the first ever arrest of a cybercriminal took place, about which it became known to the public – this is evidence of the existence at that time of the foundations of legislation on cybercrime;

4 the adoption in the USA of the first in world history 'computer' law.

We propose to name this historical period a stage of transnational cybercrime and cyberterrorism, since the next stage in the development of computer crime is associated with its access to the international level and the appearance of signs of targeted use of terror on a large scale. The emergence of the phenomenon of cyber-terrorism dates back to 1998, when a 12-year-old hacker hacked into a computer system that controlled the drainage of a dam in Arizona, which in the future could lead to the flooding of two cities at once. Therefore, we state that at the third stage a significant aggravation of the situation with cybercrimes occurred. They acquired such threatening forms that, in addition to the stability of the world financial system, they began to threaten people's lives and health. Drawing parallels with the subject of our research, this stage showed the need for more stringent regulatory measures to combat cybercrime. As we noted, if at the previous stage cybercriminals could receive a conditional sentence, then new realities showed that such sanctions do not correspond to the degree of danger of the committed acts.

Therefore, the stage of transnational cybercrime and cyber terrorism is characterised by the following features:

1 advent of international cybercrime

2 advent of new forms of cybercrime, which contained signs of terror

3 the discrepancy between the existing sanctions for computer crime and the danger of actions.

Now there is the last stage of development – the stage of the emergence of new forms of computer crimes. Among them it is worth noting the following:

1 internet war – for the first time groups of computer activists, condemning hostilities in Yugoslavia and NATO, hacked government computers and spread anti-war internet propaganda

2 internet strike is a group activity that leads to an overload of the internet site and the impossibility of its visiting by other users, etc.

Obviously, such a list of new forms is far from exhaustive, but the main purpose of its presentation is to demonstrate that the issues of legal regulation of the fight against cybercrime in the world need constant evolution and improvement, because computer criminals are constantly changing directions and methods of their activities. Therefore, the main features of the modern stage are:

1 the evolution of cybercrime, the emergence of its new forms

2 the attempts of legislators to adequately respond to these changes.

4 Results and discussion

4.1 Stages of the legal regulation of the fight against cybercrime

As a result of the analysis of the legal doctrine, we have identified the following stages in the development of the phenomenon of cybercrime:

1 The preparatory stage (the beginning of the 60s – the beginning of the 70s of the XX century) – the initial moment should be considered the first cases of crimes committed with the use of electronic computers; at the end, computer attackers were already organised criminal groups who used their knowledge for illegal enrichment and violation of the established order.

2 The spread of cybercrime (the beginning of the 70s of the 20th century – 1986) – the emergence of hackers and their organised groups should be considered as the beginning, and the completion should be associated with the adoption of the first in the history of the regulatory act on cybercrime and the first in the history of hacker arrest.

3 The stage of transnational cybercrime and cyber terrorism (1994 – the beginning of the XXI century) – the initial moment of this stage is associated with the 'Vladimir Levin case', the first major international transnational networked computer crime, and the final date was chosen conditionally – we carried out its binding to the beginning of the new century in which no significant historical events took place in the development of cyber-terrorism, but in which there is a planned evolution of computer crime.

4 The current stage of cybercrime (XXI century) – the stage of the emergence of new forms of computer crimes.

Thus, we have established that the genesis of development and the genesis of the legal regulation of the fight against cybercrime cannot be identified. Cybercrime is developing in accordance with the evolution of the latest technologies, so today it is an area that is constantly one step ahead of its regulatory framework. Taking as a basis the phasing of development, we note that in the first two stages, the legislative regulation of this institution was not actually carried out at all. Thus, we have given an example of cybercrime, as a result of which the first detention of hackers occurred, but their conditional punishment indicates the absence of adequate tools to combat computer criminals at that time. Accordingly, in the second and third stages, the legal regulation of the fight against cybercrime in the world has already been fully implemented.

As we established, 1986 is the date of the adoption of the first ever computer law, the Computer Fraud and Abuse Act in the USA. However, it is worth noting that at that time there was already a development of a legal framework aimed at preventing and suppressing cybercrime in different countries of the world. For example, the corresponding changes in domestic criminal law were made by Canada in 1985, Germany in 1986, Japan in 1987, and a little later – by England in 1990, Ireland, Portugal and Turkey in 1991, Luxembourg and the Netherlands in 1993, Israel in 1995, Belgium in 2000. The significant acceleration of this process after 1990 explains the adoption of Recommendation No. R (89) 9, approved by the EU Committee of Ministers on 13.09.1989, which was developed from 1985 to 1989 by the Council of Europe Special

Committee of Experts on Computer-related Crime (Recommendations, 2004). The role of Recommendation No. R (89) 9 is significant, since this document has had a great influence on the development and change of legislation in European countries. The recommendation enshrines the list of crimes that was recommended for the development of a unified strategy for the fight against cybercrime by the member states of the European Union. In addition, the document points out the need to achieve international agreement on the criminalisation of individual computer crimes. The recommendation contains two lists of crimes – 'minimum' and 'additional'. The minimum list included actions that must necessarily be prohibited by international law and are subject to prosecution, and an additional list formed offenses in which the achievement of international agreement is not always possible. Thus, the first stage of the genesis of legal regulation of the fight against cybercrime will be limited to the period from 1986, that is, the adoption of the first ever computer law, until 1989, when the adoption of Recommendation No. R (89) 9 took place, which had a significant impact on the further development of legislation on cybercrime and triggered changes in criminal law in European countries. So, after 1989, a rapid evolution of the criminal legislation of European states began in terms of strengthening the fight against computer crimes, which to some extent continues to this day.

Summing up, the first stage of the genesis of the legal regulation of the fight against cybercrime in the world is characterised by the following features:

1 the adoption of the first in the history of 'computer' law

2 introduction of changes in domestic criminal laws by some countries

3 the adoption of recommendations for European countries to combat cybercrime, which subsequently largely influenced the rapid evolution of European legislation.

The value of the initial stage lies in the fact that at the time of its inception, cybercrime had already reached a threatening scale and was developing rapidly. The adoption of the first regulatory acts did not affect the decrease in the volume of computer crime, however, it demonstrated the will of the leading states of the world to combat this negative phenomenon.

Therefore, the year 1989, in our conviction, serves as the starting date for the next stage of the genesis of legal regulation of the fight against cybercrime in the world – amending the criminal legislation of European countries, which conditionally lasted until 2000. The use of the term 'conditional' is due to the fact that this process as a whole continues to this day. However, firstly, given the analysis of the dynamics of adoption of changes in domestic criminal legislation by states at this stage, it should be concluded that it was in 2000 after Belgium adopted amendments to criminal legislation that further changes to national legislation did not have such a mass character. Secondly, the year 2000 marks the beginning of the adoption of important international legal acts, which today form the basis of European and world cybercrime legislation.

These international legal instruments in the matter of legal regulation of international relations in this area include the United Nations Convention against Transnational Organized Crime of 11/15/2000 (2000), the Vienna Declaration on Crime and Justice: Responses to the Challenges of the 21st Century (UN) of 04/17/2000 (2000), European Convention on mutual assistance in criminal matters between the Member States of the European Union (1962), International Convention on Cybercrime (2001), Additional

Protocol to the Convention on Cybercrime (2003), which concerns the criminalisation of racist and xenophobic acts committed through computer systems, an agreement on cooperation of the Commonwealth of Independent States in the fight against crimes in the sphere of computer information (2001), a number of other documents, such as the Council of Europe recommendations.

Thus, in fact, over the course of two years, a number of acts appeared in international law, which largely had an impact on the fight against cybercrime. That is why the third stage of the genesis of legal regulation of the fight against cybercrime in the world, we gave the name 'consolidation of the European community' and chronologically limited it to only two years – 2000 and 2001. At present, this stage should be considered as a key, since at previous ones, correlating the pace of development of cybercrime and tools of legal regulation of fighting it, computer criminals were always ahead. However, since the beginning of the 21st century, developed countries and the European community have demonstrated their willingness to take tough measures to overcome computer crime as a phenomenon. So, the third stage of the genesis of the legal regulation of the fight against cybercrime in the world is characterised by the following features:

1 the dynamic evolution of the national legislations of the leading states of Europe and the world in terms of enhancing criminal responsibility for committing computer crimes

2 adoption of basic international legal acts on cooperation and mutual assistance of the leading states of the world in cyber security issues, which today constitute the legislative basis in the field of combating cybercrime

3 legislators have reached a qualitatively new level in the fight against computer criminals due to the strengthening of interstate relations and the expansion of the content of the concept of 'cybercrime'.

Regarding the next period, which is the last, in our opinion, it is the current stage of the legal regulation of the fight against cybercrime, which continues to this day. This period can be characterised, given the specific significant events that have occurred or are occurring – its main characteristic is the improvement of legislation on cybercrime of states that are several steps behind developed countries on this issue. These states, in particular, include the Republic of Kazakhstan. Highlighting the specific signs of the modern stage, we note the following:

1 international legislation has not changed significantly, but gradually evolves

2 the involvement of an increasing number of countries in the fight against cybercrime.

Thus, the study of the genesis of the legal regulation of the fight against cybercrime in the world requires the allocation of its own historical classification. In the process of analysing the scientific doctrine, we have established that the question under study should be phased out as follows:

1 The stage of inception of the legal regulation of the fight against cybercrime (1986–1989) – from the adoption of the first ever computer law to the adoption of Recommendation No. R (89) 9, which was of as a key importance for the further development of legislation aimed at combating cybercrime and acted as an impetus for the evolution of European criminal legislation.

2 The stage of amending the criminal legislation of European countries (1989–2000) – after 1989, a rapid evolution of the criminal legislation of European countries began in terms of strengthening the fight against computer crimes, which to some extent continues to this day, and the deadline for this period we conditionally associate with the year 2000, after which further changes in national legislations were no longer characterised by a mass character.

3 The stage of consolidation of the European community to combat cybercrime (2000–2001) over the course of two years, a number of acts appeared in the international legal legislation that largely had an impact on the fight against cybercrime. That is why this stage is chronologically limited to only two years.

4 The current stage of legal regulation of the fight against cybercrime (2001–our day) – is characterised by the process of improving the legislation on cybercrime of states that are at the lowest levels of development.

4.2 Current international legal regulation of the fight against cybercrime

The international legal regulation of the fight against cybercrime plays an extremely important role due to the transboundary nature of the relevant crimes, the difficulty of searching for the perpetrators and customers of such unlawful criminal acts, the need to apply modern technical and information technologies, and contribute to the activation of international legal acts on these issues. Sources of international legal regulation of the corresponding circle of public relations can be divided into two large groups:

1 universal sources

2 regional sources.

In modern conditions, the United Nations has taken on a coordinating role in developing both conceptual and legal frameworks for the regulation of as a key issue in the fight against cybercrime. The growth of the relevant type of crime, the nature and severity of the crimes committed, and others, requires an immediate response from the international community to the corresponding negative social manifestations. It is under the auspices of the UN, which brings together the largest number of countries in the world, it is advisable to carry out activities to develop and implement international legal regulation of the studied public relations. The adoption of the relevant resolution, which outlined the framework agreements, was one of the first steps towards the creation of an international legal framework on the fight against cybercrime.

The relevant discussion contributed to the development of international legal cooperation in the fight against cybercrime, but the disadvantage of the relevant event was that it focused on computer crimes, while information crimes were much broader and also covered electronic communications, electronic networks, etc. The content of the relevant document declares quite progressive provisions, but its significant drawback is that for a full-fledged activity on countering cybercrime, a significant number of states of the relevant processes are required, only under such conditions it is possible to achieve the desired result. Therefore, the relevant policy document, although it was the basis for the development of the following regulatory documents, however, does not play a significant role in the international legal regulation of the fight against information crime.

Subsequently, within the framework of the UN, relevant activities were carried out in such areas as:

1 combating the criminal use of information technologies

2 international information security

3 the creation of a global culture of cybersecurity and the protection of critical information structures.

Important issues of state cooperation in combating the criminal use of information and communication technologies were entrusted to the International Telecommunication Union. The result of the activity was the adoption by the said subject of the Global Cybersecurity Program, which defined the goals, principles and strategies for developing models of legislation in the field of combating computer crime. The priorities of the global program were:

1 the formation of strategies for the development of model legislation to combat cybercrime, which can be applied on a global scale and which will be compatible with existing national and regional legislation

2 the formation of global strategies to create appropriate national and regional organisational structures, as well as policies to combat cybercrime

3 development of a strategy for establishing globally acceptable minimum security criteria and authorisation schemes for hardware, software applications and systems

4 developing strategies for creating a global framework for monitoring, alerting and responding to incidents to ensure international coordination of activities

5 development of global strategies for the creation and approval of a common and ad hoc digital identification system, as well as the necessary organisational structures for the recognition of digital identity cards without taking into account geographic boundaries

6 the development of a global strategy to promote the development of human and institutional capacities to increase knowledge and know-how

7 preparation of proposals based on a global strategy based on the participation of multi-stakeholders in order to foster international cooperation, dialogue and coordination of activities.

Subsequently, a number of ITU resolutions were adopted to implement the planned activities, which were aimed at strengthening confidence and security in the use of information and communication technologies and the fight against computer crime.

Features of the universal international legal regulation of the fight against cybercrime is the following:

1 the relevant activity is accumulated around the United Nations and its bodies or subjects created with its support

2 today there are only program and other strategic documents that should lay the foundation for the international legal regulation of the relevant circle of relations

3 the main activities should be the creation and development of organisational and legislative measures to counter cybercrime, as well as issues of interaction in this field of activity

4 there is a need for the establishment of international joint bodies of operational search activities to ensure the fixation of traces of the crimes committed

5 improvement of interaction between the competent authorities of different states

6 there is an urgent need for the development and adoption of universal conventions on relevant issues that would ensure the participation of most states in relevant activities against cybercrime.

The legislation of the European Union in the field of information security developed in line with international initiatives of the Council of Europe, the Organization for Economic Cooperation and Development, the International Telecommunication Union, the United Nations. Legislative measures to combat cybercrime were carried out within the framework of the programs of the European Union – 'Secure Internet' (1999–2004), 'Secure Internet Plus' (2005–2008), 'Secure Internet 2009–2013', adopted by European Parliament and the Council, and mainly focused on the protection of personal data, promoting the safe use of the internet, creating a favourable environment for the development of the European internet industry, the protection of children using the internet and new information technologies. The most important measures to combat cybercrime were carried out within the framework of the European Union's Crime Prevention and Crime program and included cooperation in countering cybercrime. The complexity and number of information security issues has formed in the legislative bodies of the European Union a conceptual vision of the future international legal regulation exclusively at the level aimed at solving criminal aspects related to the use of information and communication technologies. In the European Union, the concept of international information security, which would provide a comprehensive solution to the problem at three levels of international legal regulation – military, terrorist and criminal, was not perceived.

The leading place among the relevant group of international legal documents is reserved for the Council of Europe Convention on Cybercrime of 23 November 2001 (Budapest). The Republic of Kazakhstan plans to ratify it in 2020. Today it is one of the most important documents regulating legal relations in the global computer network and is still the only document of this level. According to it, states are obliged to adopt legislative and other measures that may be necessary to establish criminal in accordance with its domestic legislation for crimes in cyberspace.

The Convention on Cybercrime is one of the most important documents in the global computer network, whose role in regulating the fight against cybercrime in states around the world is crucial. Regarding the Republic of Kazakhstan, the significance of this international legal act can be expressed as follows. First, the convention distinguishes crimes depending on the object of encroachment on:

1 offenses against the confidentiality, integrity and availability of computer data and systems

2 computer related offenses

3 content-related offenses

4 offenses related to violation of copyright and related rights.

Similarly, such offenses are also classified in the national legislations of the participating countries, in particular in Section X of the Criminal Code of the Republic of Kazakhstan (2014). Secondly, the Convention regulates procedural aspects, such as conditions, preventive measures, search and seizure of computer data that is stored, collection of data on the movement of information in real time, interception of information content data, jurisdiction, and the like. Such systematisation greatly facilitates the activities of state law enforcement agencies. Thirdly, this document establishes the principles of cooperation of the participating countries in the field of combating cybercrime, in particular – extradition and mutual assistance. Note that the implementation of this aspect is carried out by the conclusion of bilateral agreements by states. As their analysis has already shown, in practice the Republic of Kazakhstan prefers the implementation of the principle of mutual assistance. Fourthly, the Convention grants the right of participants to access publicly accessible computer data that is stored without obtaining permission from the other party, which greatly facilitates the investigation of crimes and avoids undue delay in investigative activities.

The Convention on Cybercrime is an important basis for the activities of the police of the Republic of Kazakhstan, however, some of its provisions have not been reflected in domestic criminal legislation. For example, production, sale, purchase for use, import, wholesale or other forms of provision of computer passwords, access codes or other similar data through which the computer system as a whole or any part of it can be accessed with the intention of using it for the purpose of committing computer crimes were not embodied in the domestic criminal law. The problem is that, on the one hand, law enforcement officers are empowered to control the norms of the Convention on Cybercrime in their activities, but on the other hand, in practice, they almost do not use them, so transferring international standards to the domestic practice of fighting cybercrime is not fully correct. However, despite such contradictions, the Convention on Cybercrime is still one of the most important instruments of national legal regulation of the fight against cybercrime.

The United Nations Convention against Transnational Organized Crime of 11/15/2000 is not a regulatory act that directly regulates the fight against cybercrime. However, computer crime is predominantly transnational in nature, is organised and can acquire signs of terrorism. Consequently, the adoption of the Convention aimed at preventing and combating these types of criminal acts is an important tool in the fight against cybercrime.

The United Nations Convention against Transnational Organized Crime of 15 November 2000 proposed the adoption of legislative and other measures aimed at measures against corruption and the liability of legal entities for participating in serious crimes involving organised crime; measures that can provide opportunities for confiscation and seizure of proceeds from crime and disposal of confiscated proceeds from crime, and the like. The provisions of the Convention do not apply to offenses that are not related to organized crime, considering, as an exception, only certain areas – especially computer offenses, since this problem requires more attention from the international community. That is, if a cybercrime is transnational in nature, namely, it is planned or committed in several states, or is committed in one state, and has significant consequences in another, the norms of the Convention can be applied.

It is worth noting that the total number of international treaties in the field of cooperation in criminal matters is significant. Ever since the declaration of independence, the Republic of Kazakhstan has actively concluded similar agreements and cooperates with several dozens of states from different continents. However, most of them do not regulate in any way cooperation in the field of combating cybercrime, which generally does not exclude such a possibility if the need arises. This indicates that specific cooperation in the fight against cybercrime is not provided, however, it is not excluded if such problematic issues arise.

The Agreement on Cooperation of the States Parties of the Commonwealth of Independent States in Combating Computer Crime Offenses of 1 June 2001 imposes on States obligations to recognise, in accordance with national legislation, as criminal offenses:

1 the implementation of unauthorised access to computer information protected by law, if this was followed by the destruction, blocking, modification or copying of information, disruption of the computer, computer system or their network

2 the creation, use or distribution of malicious programs

3 violation of the rules of operation of a computer, computer system or their network by a person who has access to a computer, computer system or their network, resulting in the destruction, blocking or modification of computer information protected by law, if this entailed significant harm or serious consequences

4 illegal use of computer programs and databases that are objects of copyright, as well as the assignment of authorship.

However, for the full implementation of the relevant tasks it was necessary to agree on a clear list of relevant criminal acts and punish them. In practice, not all states that are members of the CIS, have implemented the relevant tasks, which significantly reduces the counteraction of information crime, which requires complex transnational cooperation.

In the agreement between the governments of the Shanghai Cooperation Organization member states on cooperation in the field of international information security, adopted on 16 June 2009, information crime issues are considered in the general context with the main directions, principles, forms and mechanisms of international cooperation. It is worth noting that, unlike the previous ones, the Agreement provides for a new conceptual approach to the issues of ensuring international information security. Its essence lies in the complex provision of the international information security of states against all information threats that may be caused by the criminal use of ICT. Based on these positions, information crime, along with five others, is recognised by the parties to the transaction as the main threat in the field of ensuring international information security. The source of this threat, according to the agreement, is individuals or organisations engaged in the misuse of information resources or unauthorised interference with such resources for criminal purposes.

In order to counter information crime, the parties to the transaction agreed to cooperate and conduct their activities in the information space in such a way that such activities contribute to social and economic development and are compatible with the objectives of maintaining international security and stability, consistent with generally accepted principles of international law. Such activities must be compatible with the right

of each party to the Transaction to seek, receive and disseminate information, taking into account possible restrictions for reasons of protecting the interests of national and public security (Article 4). The parties recognised the right to protect information resources and critical structures from unauthorised use and unauthorised interference, agreed not to carry out such actions against each other and assist each other in the realisation of this right. A significant drawback of the relevant international legal document was that, despite declaring the need to combat cybercrime, it does not contain real measures. That is, there are no obligations of the member states to amend national legislation that would contribute to a real counteraction to information crimes. The essence of the relevant document is reduced to the characteristics of threats of information crimes, the need to consolidate the efforts of states, and the like.

As part of the Asia-Pacific Economic Community, the APEC Cybersecurity Strategy was adopted in 2002, it is planned to adopt a code of laws on cyber security and cybercrime, as well as the creation of national cybercrime units and technological assistance centers. The League of Arab States and the Organization of American States are developing cooperation in the fight against computer crimes, taking into account the recommendations of the UN, ITU, the Council of Europe.

The activities of the Organization for Economic Cooperation and Development, started on the subject of computer crime back in 1983, are directed to conduct research related to the possibility of harmonising criminal legislation in relation to computer crimes. In 1992, the OECD Council adopted Guidelines for Information Security. In 2002, a new version of the principles 'OECD Guidelines for Ensuring the Security of Information Systems and Networks: Towards a Security Culture' was recommended by the OECD Council. The latest reports were on anti-spam topics (2005), and legislative decisions of states on the problem of cyber-terrorism (2007).

5 Conclusions

The features of regional international legal regulation of countering cybercrime can be defined as follows:

1 considerable attention from various regional international organisations to countering cybercrime

2 development of numerous regional agreements on cooperation in the field of countering information crimes

3 the relevant activity is at the stage of its inception, since most of the documents began to be formed in the late 1990s – in the early 2000s

4 such activity is an integral part of both international information relations and criminal proceedings.

The study gives grounds to assert that to create the conditions for proper and effective activities to counter cybercrime there are not enough resources of one law enforcement agency or law enforcement agencies of the Republic of Kazakhstan. Such activities should be comprehensive and involve many countries, which requires the necessary legal framework at the international level. Today, actions are underway to establish the foundations of international cooperation in the area of countering cybercrime within the

framework of both universal and regional treaties. At the same time, such measures for full-fledged activities are not enough, which requires the revitalisation of activities on the part of each subject of the international community in order to create an effective mechanism of international legal regulation of countering cybercrime.

References

Additional Protocol to the Convention on Cybercrime (2003) *Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems* [online] https://rm.coe.int/168008160f (accessed 15 July 2019).

Agreement on Cooperation of the States Parties of the Commonwealth of Independent States in the Fight Against Crimes in the Field of Computer Information (2001) [online] http://base.garant.ru/12123778/ (accessed 15 July 2019).

Allum, F. and Sands, J. (2004) 'Explaining organized crime in europe: are economists always right?', *Crime, Law and Social Change*, Vol. 41, No. 2, pp.133–160.

Beken, T.V. (2004) 'Risky business: a risk-based methodology to measure organized crime', *Crime, Law and Social Change*, Vol. 41, No. 5, pp.471–516.

Bergeron, J. (2013) 'Transnational organised crime and international security: a primer', *RUSI Journal*, Vol. 158, No. 2, pp.6–9.

Blum, J.A. (1997) 'Enterprise crime: financial fraud in International Interspace Working Group on Organized Crime, National Strategy Information Center Washington, DC, June 1–31, 1997', *Trends in Organized Crime*, Vol. 3, No. 1, pp.115–120.

Boylan, S.P. (1997) 'Organized crime and corruption in russia: implications for US and international law', *Trends in Organized Crime*, Vol. 3, No. 1, p.40.

Calderoni, F. (2011) 'Tom Obokata: transnational organized crime in international criminal law', *European Journal on Criminal Policy and Research*, Vol. 17, No. 4, pp.347–348.

Criminal Code of the Republic of Kazakhstan (2014) 3 July 2014, No. 226-V, with amendments and additions as of January 21, 2019 [Online] https://online.zakon.kz/Document/?doc_id=31575252 (accessed 15 July 2019).

Edwards, A. (2001) 'Global organized crime and international security', *Security Journal*, Vol. 14, No. 1, pp.77–78.

European Convention on Mutual Assistance in Criminal Matters (1962) [online] https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/030 (accessed 15 July 2019).

Finckenauer, J.O, and Chin, K. (2006) 'Asian transnational organized crime and its impact on the United States: developing a transnational crime research agenda', *Trends in Organized Crime*, Vol. 10, No. 2, pp.18–107.

Hagan, F.E. (2006) ''Organized Crime' and 'organized crime': indeterminate problems of definition', *Trends in Organized Crime*, Vol. 9, No. 4, pp.127–137.

International Convention on Cybercrime (2001) *European Convention on Cybercrime* (crimes in cyberspace), Budapest, 23 November 2001 [online] https://rm.coe.int/1680081580 (accessed 15 July 2019).

Kramer, R.C. (2016) 'State-organized crime, international law and structural contradictions', *Critical Criminology*, Vol. 24, No. 2, pp.231–245.

Kryvoi, Y. (2018) 'Economic crimes in international investment law', *International and Comparative Law Quarterly*, Vol. 67, No. 3, pp.577–605.

Leonov, D., and Ayaganova, S. (2018) 'Issues of improving the legislation of the republic of Kazakhstan based on the international standards on counteraction to crimes connected with human trafficking', *Journal of Advanced Research in Law and Economics*, Vol. 9, No. 3, pp.1026–1033.

Levi, M. and Maguire M. (2004) 'Reducing and preventing organised crime: an evidence-based critique', *Crime, Law and Social Change*, Vol. 41, No. 5, pp.397–469.

Recommendations (2004) *20 of the Committee of Ministers of the Council of Europe to Member States on Judicial Review of Administrative Acts* (adopted by the Committee of Ministers on 15 December 2004 at the 909th meeting at the level of permanent representatives) [online] https://vgmu.hse.ru/2009--2/26547901.html) (accessed 15 July 2019).

Schroeder, U.C. and Friesendorf, C. (2009) 'State-building and organized crime: implementing the international law enforcement agenda in Bosnia', *Journal of International Relations and Development*, Vol. 12, No. 2, pp.137–167.

Shelley, L.I. and Picarelli J.T. (2005) 'Methods and motives: exploring links between transnational organized crime and international terrorism', *Trends in Organized Crime*, Vol. 9, No. 2, pp.52–67.

Tripp, T.M. and McMahon-Howard, J. (2016) 'Perception vs. reality: the relationship between organized crime and human trafficking in metropolitan Atlanta', *American Journal of Criminal Justice*, Vol. 41, No. 4, pp.732–764.

United Nations Centre for International Crime Prevention (2000) 'Assessing transnational organized crime: results of a pilot survey of 40 selected organized criminal groups in 16 countries', *Trends in Organized Crime*, Vol. 6, No. 2, pp.44–92.

United Nations Convention against Transnational Organized Crime (2000) *Adopted by General Assembly Resolution 55/25 of 15 November 2000* [online] http://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml (accessed 15 July 2019).

United States Code (2017) [online] https://www.law.cornell.edu/uscode/text/18/1030 (accessed 15 July 2019).

Van Dijk, J. (2007) 'Mafia markers: assessing organized crime and its impact upon societies', *Trends in Organized Crime*, Vol. 10, No. 4, pp.39–56.

Vienna Declaration on Crime and Justice: Responding to the Challenges of the 21st Century (2000) *Adopted at the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, Vienna, 10–17 April 2000 [online] http://www.un.org/ru/documents/decl_conv/declarations/vendec.shtml (accessed 15 July 2019).

von Lampe, K. (2006) 'The interdisciplinary dimensions of the study of organized crime', *Trends in Organized Crime*, Vol. 9, No. 3, pp.77–95.

Williams, P. and Godson, R. (2002) 'Anticipating organized and transnational crime', *Crime, Law and Social Change*, Vol. 37, No. 4, pp.311–355.

Zhuravel, V.A. and Kurumisawa, Y. (2019). 'Criminalistics in the system of scientific knowledge', *Journal of the National Academy of Legal Sciences of Ukraine*, Vol. 26, No. 2, pp.85–97.

Zysset, A. (2018) 'Right, crime, and court: toward a unifying political conception of international law', *Criminal Law and Philosophy,* Vol. 12, No. 4, pp.677–693.