The Specifics and Patterns of Cybercrime in the Field of Payment Processing

Boris Sturc[1,*], Tatyana Gurova[2] and Sergei Chernov[3]

[1]*University of Economics in Bratislava, Bratislava, Slovakia*

[2]*Moscow City Teachers' Training University, Moscow, Russian Federation*

[3]*State University of Management, Moscow, Russian Federation*

Abstract: In the modern world, cybercrime in the field of payment processing as a phenomenon is developing rapidly. Highly developed, developing and least-developed states become victims of cyberattacks. The purpose of this study is to analyze the experience of the international community and a number of states in combating cybercrime in the field of payment processing. International and regional (on the example of the Council of Europe) legal regulation of the fight against this type of crime were analyzed. The data on the size of losses caused by cybercrime to the world economy are analyzed according to the latest report from the Center for Strategic and International Studies for 2018, the World Economic Forum for 2019, DLA Piper GDPR for the period January-April 2020. Besides, using the example of the Russian Federation, quantitative indicators of the growth of cybercrime and the level of its detection for the period from 2018 to April 2020 were investigated. Comparison of the experience of individual states and its analysis made it possible to single out the best possible measures to counter cybercrime in the field of financial processing. The necessity of interstate cooperation to counter cybercrime in the field of payment processing is indicated. However, due to the presence of significant differences in the legal systems of all states, it is proposed to interact within the framework of regional communities with gradual transfer to international interaction. The priority is given to precisely preventive measures to counter cybercrime in the field of payment processing.

Keywords: Cybercrime, cybersecurity, Internet technologies, payment processing, preventive measures against cybercrime.

INTRODUCTION

Currently, the country's level of development is determined by the availability of advanced information technologies (Klochkova, Tyurina, Chernov 2019). Internet technologies are an integral part of life, a sphere of human information activity that is developing rapidly (Korobeyev, Dremlyuga, and Kuchina, 2019). currently, seemingly, the vast majority of people use the Internet. As of 2019, in comparison with 2018, the number of users of this network increased by 5.3%, while compared with 2009 (25.8%) - by 27.8% (in 2019, the figure was 53.6% of the total population of the planet). In addition, in 2019, in developed countries, nearly 87% of the total population used the Internet, while in the least developed countries, 19% of the population (International Telecommunication Union 2019). On the one hand, this indicates a significant development and expansion of the Internet. On the other hand, the population and social institutions of developed countries are more integrated into the Internet than the population and social institutions of the least developed countries. Moreover, in the modern world, many state and public institutions are even integrated into the Internet. For example, public administration functions are implemented by state authorities and local governments through the use of various web platforms (for example, e-government, e-health, e-education) (Jain 2020).

At the same time, expanding the range of activities carried out with the help of the Internet has also increased the number of new types of crimes such as phishing, card fraud, etc. Today, cybercrime is no longer an internal state problem but an international one, since activities, including criminal ones, carried out on the Internet cannot be limited to the framework of one state (Yakimova and Narutto 2016). Cybercriminal activity is characterized by generating income from embezzlement of funds in a different way, receiving income from the sale of confidential, commercial or other valuable information obtained in an illegal way, as well as other types of cybercrime. At the same time, law enforcement agencies are often powerless against this problem due to the high latency of cybercrime. The low detection rate of cybercrime is facilitated by the mismatch of methods, technologies used by law enforcement officers, the level of innovative methods used by criminals (Jain 2020; Nagurney 2015). As of today, cybercrime is a heterogeneous criminal activity. It is presented in various forms, the key ones being hacking (meaning black hacking, that is, hacking a program or system to steal the information there), theft of personal data and a denial of service attack. The latter, also known as a

*Address correspondence to this author at the University of Economics in Bratislava, Bratislava, Slovakia; E-mail: b_search57@yahoo.com

E-ISSN: 1929-4409/20

DoS attack, has as its goal the creation of conditions under which the access of system users to the provided resources of the system will be either blocked, impossible, or difficult (Orji 2019).

On the one hand, there is actual impossibility of users to refuse to make various Internet payments and various kinds of other money transfers for goods or services using special terminals. At the same time, the targets of cybercriminals' attacks are not only private individuals, but also various banking and financial organizations, software manufacturers, information security departments of states, the states themselves, as well as a number of other entities.The issue of solving the problem of effectively combating cybercrime, as well as improving the competence of law enforcement agencies in countering such criminal activities, is on the agenda. Moreover, first of all, such a question arises among highly developed states (Raghavan and Parthiban 2014; Leukfeldt 2014), then among developing ones (Korobeyev *et al*. 2019; Ospanov, Nurusheva, and Nurushev 2019) and least of all in least developed countries (Mugari, Gona, Maunga, and Chiyambiro 2016).The Russian Federation is one of the developing countries, but it is one of the Commonwealth of Independent States (CIS) countries. Within the CIS, it is at the forefront of cybersecurity (Global Cybersecurity Index (GCI) 2018). As of 2018, 68418 cybercrimes have been registered in the Russian Federation; 416933 facts of unauthorized operations with payment cards in the amount of 1384.7 million rubles (Lakomov 2019). At the same time, the total number of crimes committed using information and telecommunication technologies (ICTs) as of 2018 amounted to 174674 facts of crimes. At the same time, in January-October 2019, there were already 240209 such crimes (Nazmeyeva 2020). For the period 2015-2020, the number of cases of cybercrime in the Russian Federation increased from 11 thousand to 295 thousand cases, that is, in fact, by 25 times, which confirms the gradual increase in the number of committed cybercrime activities. Although in 2019 the rate of detection of cybercrimes increased by 1.5 times, the overall level of detection was only 9% of the total number of crimes (Korobeyev *et al*. 2019). Besides, criminals have a high level of adaptation, while law enforcement agencies are always less adapted, since the bureaucratic nature of the state leads to the difficulty of introducing innovations into its functioning as a whole.

Payment processing is directly related to the concept of electronic commerce, which includes the sale of services, goods through the Internet and is not limited to payments and transfers only (Lakomov 2019). The payment processing itself, or payment service, is one of the structural units of electronic commerce. Its purpose is to ensure the possibility of exchanging data between the participants in the process, as well as closing the transaction by transferring funds by debiting funds from the buyer's account and crediting them to the seller's account, on the one hand, and transferring goods or services from the seller to the buyer. Today, the subjects of payment processing are both national and international payment systems. At the same time, the regularity of cybercrime in the field of payment processing is increasing. The purpose of this work is to identify patterns and characteristics of cybercrime in the field of payment processing, as well as to find ways to prevent and combat it effectively. To this end, an analysis was made of the experience of preventive measures and combating cybercrime of international community as a whole and the European Union (EU) as the brightest integration political unit, on the one hand, and the United States (USA), Germany, the Russian Federation, the Republic of Kazakhstan, Zimbabwe and a number of other states as national jurisdictions, on the other. In addition, potential obstacles to the effective prevention and combating of cybercrime in the field of payment processing were pointed out (Chernov 2016).

METHODOLOGY

In this study, the experience of preventing and combating cybercrime in the field of payment processing was analyzed. The experience of international and regional (by the example of the Council of Europe) communities was taken into account. The experience of a number of states was also taken into account. The analysis was carried out on the principle of dividing the states under consideration into highly developed, developing and least developed. The emphasis was primarily on organizational measures to prevent and combat cybercrime in the field of payment processing. This approach allowed comprehensively studying the nature of such a phenomenon as cybercrime in the field of payment processing. In the framework of this work, the norms of such key international acts as the United Nations Convention against Transnational Organized Crime (UNTOC), as well as the Council of Europe Convention on Cybercrime (CETS No. 185), were analyzed.

The data of the latest reports of the Center for Strategic and International (CSIS) Studies for 2018, the World Economic Forum (WEF) for 2019, the DLA Piper GDPR for the period January-April 2020 were studied. Studies of statistics on losses caused by cybercrime to the global economy have shown how cybercrime is developing and how the size of the losses caused by it grows. The analysis of statistical data on the example of the Russian Federation for 2018 - April 2020 indicated a disproportion in the number of registered cybercrimes and the number of court proceedings.

Overall, The Payments industry remains a lucrative target for financially-motivated actors. Payment systems, the network of infrastructure that it relies on and the organizations that own or protect them are all at risk of being viewed for potential vectors of attack. Hence, we set out to establish an analysis to make it possible to single out the best possible measures to counter cybercrime in the field of financial processing.

Through the application of the conceptual method, the most effective measures to counter cybercrime in the field of payment processing were identified. Using the comparative method, the organizational methods of combating cybercrime in the field of payment processing in the countries cited in the study were investigated. In particular, the features of the interaction of law enforcement agencies with other state bodies and private companies (including providers) were compared. Organizational approaches to creating educational programs for law enforcement officers, on the one hand, and employees of security sectors of banking and financial companies, as well as individuals, on the other, were analyzed.

RESULTS

The Nature of Cybercrime

Cybercrime is a criminal or malicious activity of informational, global and network nature. However, cybercrime is distinguished from other crimes related to the use of computer technology. Such crimes are products of network technologies that have been transformed by criminal actors with the aim of committing and using completely new forms of crime. These include the misappropriation of information, as well as the manipulation of information and its value in networks in order to obtain benefits, for example, blackmailing specific individuals with the aim of obtaining a ransom. Cybercrime includes a wide range of activities using information technology. The same applies to cybercrime in the field of payment processing. It should be noted that the terms ‘cybercrime’ and ‘offense in the field of cyberspace’ are not identical. The latter is a broader concept, including cybercrime, which is characterized by high social danger and harmfulness. This makes it possible to distinguish them, for example, from administrative offenses in the field of cyberspace, if such are provided for in the relevant regulatory legal acts of a state (Jain 2020; Nagurney 2015).

In this case, the objects of cybercrime are various enterprises that are engaged in information security, being the key opponents of criminals. In addition, various types of banking and financial enterprises, as well as non-financial enterprises and individuals, are interesting to criminals (Jain 2020; Nagurney 2015). In particular, in practice, cybercrime is associated with traditional types of criminal activity, such as terrorism, drug trafficking, money laundering, extortion through the use of computer and mobile technologies, since the use of cybernetic technologies and methods contributes to the implementation of such. At the same time, traditional crimes and cybercrimes have their own differences (WeulenKranenbarg, Holt, and Van Gelder 2019). An example is the use of social networks to engage in terrorist activities. It should be added that the digitalization of the economy that has developed in developed countries of the world contains not only opportunities for the development of society, but also threats, including in the area of countering the financing of terrorism (Chernov 2019). However, despite the possible motivation of some cybercrimes by ideology, passion, revenge, in the end, the motive for obtaining economic benefits is always traced (Leukfeldt 2014).

It should be noted that the regulations of the Council of Europe highlight two key types of cybercrime. The criterion for such a division is the understanding that, in some of them, computer data and systems are the subjects of a criminal attempt, while in others it is a direct instrument for committing a crime. The first group consists of crimes targeted at computer systems and their data, including crimes against the confidentiality, accessibility and integrity of computer systems and data. At the same time, the second - those in which computer data and computer systems are directly instruments of crime (Raghavan and Parthiban 2014). Classifying according to the specifics of the act, they are called cyber fraud, cyber pornography (dissemination of pornography on the Internet), cyber violence (that is, harm by electronic communication or contact). Besides, depending on the object, crimes

against the personality are distinguished, among which blackmail, harassment, cyber-persecution should be highlighted; illegal use of a computer, other device and software, for example, piracy; distribution of illegal materials, in particular, child pornography; theft of intellectual property; industrial espionage; financial cybercrime (Leukfeldt 2014). Among financial cybercrimes, one should note the following:

- credit card fraud by stealing information on a specific bank card from a magnetic strip, carried out at ATMs and terminals;
- obtaining information on a specific bank card by forging an email from a legal organization;
- theft of information from a computer, other device or database system by hacking or using malicious programs;
- identity theft (Leukfeldt 2014; Nagurney 2015).

For example, the essence of credit card fraud by stealing information on a specific bank card from a magnetic strip is reduced to gaining access to the user's bank account and then transferring the funds on it to another, pre-prepared, bank account (Raghavan & Parthiban, 2014).

International Experience

For the world community, modern cybercrime, in particular in the field of payment processing, is indeed a widespread problem. It has the property of continuous development, acquires new forms of existence and parasitism at the expense of citizens and states. Cybercrime activities carried out by criminal groups and organizations pose huge threats to the loss of financial and other kinds of confidential information (Nagurney 2015). In 2018, the annual loss of the global economy due to cybercrime amounted to more than $600 billion, or almost 1% of world GDP (Center for Strategic and International Studies 2018). The gradual increase of this indicator is explained by the introduction of new technologies in cybercrime, as well as the growth of its scale (Center for Strategic and International Studies 2018; 2020). According to the DLA Piper GDPR report, from May 25, 2018, to January 27, 2020, the total number of cases of unauthorized access to personal data in the Netherlands was 40647, in Germany - 37636 cases, in the United Kingdom (UK) - 22181 cases, in Ireland - 10516 cases, in France - 3459 cases, etc. In addition, the issue of cybercrime, including in the field of financial processing, is also relevant for the United States (USA), Canada and the developed countries of East Asia (World Economic Forum, 2019; DLA Piper's Cybersecurity and Data Protection Team 2020).

The UN Convention against Transnational Organized Crime is rather a general regulation treaty; it does not specify the subject of cybercrimes. In accordance with Art. 1 of the Convention, the purpose of this act is to promote the maximum cooperation of member states in the prevention and fight against transnational organized crime without determining its specific types (United Nations (UN), 2000). However, it should be noted that this convention has a key drawback - the lack of proper attention to the regulation of the crimes in cyberspace, that is, in virtual reality.

It is indicative that, within the framework of Europe, such a deficiency is compensated by the Council of Europe Convention on Cybercrime (ETS No. 185), which is a special act in relation to the aforementioned UN Convention. The Council of Europe Convention on Cybercrime (ETS No. 185) is considered the first act of international and regional levels regulating the issue of cybercrimes.Namely, it concerns crimes committed through the Internet or other computer networks. The Convention addresses issues, including the observance of copyright and responding to the facts of its violation, computer fraud, child pornography, and network security violations. In addition, the Budapest Convention provides for a list of powers to counter cybercrime, in particular computer network searches and interception. This convention is as detailed as possible, it provides a detailed list of cybercrimes, which is its substantive part. First, the detailed separation of cybercrime provided in the convention is an advanced classification for its time. Secondly, the envisaged approach to the classification of cybercrime can be considered the basis for modern developments and classifications. Thirdly, the consolidation of a specific list of cybercrimes in the convention made it possible to implement those in the laws on criminal liability of the member states of the Council of Europe to simplify the procedure for their application. Besides, its norms are divided into substantive and procedural law. In particular, the procedural part of the Convention should include the measures envisaged by the act to prevent and combat attacks, including those committed by authorized state bodies in the investigation of relevant violations, as well as questions of litigation and international cooperation of member states. Regarding cybercrime, the Convention has identified the following: unlawful access; unlawful interception; impact on data

or on functional systems; illegal use of devices; computer fraud; child pornography offenses; violation of copyright and related rights (Orji 2019).

At the same time, at the end of October 2019, the Russian Federation submitted for consideration by the first committee of the UN General Assembly the concept of a new Convention on the Use of Information Technologies for Criminal Purposes. In particular, the Russian Federation has previously attempted to adopt a new international treaty act on this issue (Convention on ensuring international information security). The United States opposes such a concept because of localization and restriction of the freedom of the Internet. However, it should be noted that even a well-drafted contractual 20-year act is not able to fully regulate relations in the field of combating cybercrime.

National Countermeasures Experience

On the issue of preventing and combating cybercrime, including in the field of payment processing, a large number of platforms and initiatives have been created at the state level. At the US federal level, in 2018, a key need was identified for providing legal and technical capabilities to specialized structures in identifying and eliminating cybercrime. In particular, there is a need for such bodies to interact with the private sector, including providers of ICTs. The federal government proposes priority actions in this area:

- popularization of reports to the authorities about known facts of cybercrime with a view to prompt response;
- updating the legislative framework on this issue to expand the powers of law enforcement agencies;
- measures to reduce threats from transnational criminal organizations in cyberspace, as well as overcoming existing problems with bringing to justice criminals abroad;
- measures to strengthen the law enforcement capacity of US partner countries to combat cybercrime (Internet Research Institute, 2019).

In the United States, various structures have been created to carry out assigned tasks in cyberspace. For example, in the United States of America (USA) in 2008, the National Cybersecurity Center was created by the NSPD-54/HSPD-23 directive. This institution is a unit within the US Department of Homeland Security. This structure is responsible for ensuring the security of government communication networks, including monitoring, collecting and exchanging information with the National Security Agency, the Federal Bureau of Investigation, the Pentagon and the US Department of Homeland Security itself (Yakimova and Narutto 2016). In addition, in 2009, the United States Cyber Command was created and, in 2018, removed from submission to the US strategic command (Yakimova and Narutto 2016).

In Germany, the Federal Criminal Police (BKA), created a project team on electronic payment systems. This project team consists of experts in the field of investigation of financial crimes, crimes on the Internet, using computer systems and confiscation of assets, in addition - experts from among the employees of the Federal Financial Supervision Authority. Firstly, the group created an information fund on electronic payment systems, which are subject to national assessment by the police. At the same time, the Council of Europe recognized the need to create such a platform at the international level. In addition, the project team also developed a wide range of substantive recommendations, among which the following should be noted:

- wide informing of police officers on the basics of the functioning of electronic payment systems, as well as training programs on financial and cyber investigations, in particular in the field of the processing;
- active cooperation of both law enforcement agencies with online service providers and with supervisory authorities, as well as supervisory authorities among themselves;
- moving the issue of control over providers to the international level;
- active discussion and study of issues of combating financial and cybercrime, in particular in the field of payment processing, at the international level (Boin, Bynander, Jann, Schulze-Gabrechten, Lodge, Lægreid, and Ryssdal 2019)

Identification of the facts of cybercrime occurs either by informing the victim or other interested person about this to the law enforcement authorities, or by independently identifying such facts by the internal affairs bodies. The latter, using legislatively regulated operational-search measures, establish the identity of

the offender and his/her whereabouts. The next step is the detention of such a criminal.

In Ireland, more than one initiative group has been created to counter cybercrime, including in the field of payment processing. One such platform is the Irish Banking Federation Hi-Tech Crime Forum, which provides information security, risk management and anti-fraud. The Forum includes several independent entities, including the Irish Police, the Northern Ireland Police, the Payment Services Organization of Ireland, the Internet Service Providers Association of Ireland and the University of Dublin Center for Cybercrime Investigation. According to the Council of Europe organization (CoE), the Forum has achieved significant success in several areas. First, approaches to identifying threats to banking and payment services based on the experience of other jurisdictions have become successful. These approaches may include: tactical and strategic forecasting to strengthen the financial stability of the banking and financial system as a whole; long-term forecasting and planning of financial security; functional analysis of the security level of banking and financial activities; permanent assessment of the achieved security level. Secondly, in establishing close cooperation and mutual trust between the Forum participants without signs of mutual competition between them. Thirdly, in work to forestall nascent cyber threats. Within the framework of this Forum, the University of Dublin's Center for the Investigation of Cybercrime, which actively interacts with the national law enforcement system and with both the international and the national private sector, should be highlighted. The Center has several tasks. Firstly, there is an active interaction at the master's level of science of law enforcement agencies both during investigations and during the data processing conducted by the Center. Secondly, the Center performs an educational function by training law enforcement specialists. Ireland's experience not only confirms the direct need for law enforcement to engage with the private sector, including Information Communication Technology (ICT) providers. This experience is also valuable in that it reflects the effectiveness of, firstly, stimulating research on countering cybercrime, and secondly, involving higher education institutions in the training and retraining of specialists in the field of cybersecurity.

Therefore, given the positive and negative experience of countering cybercrime in the field of payment processing, European states have developed priority and fundamental approaches and guidelines that form the basis for countering this type of illegal activity. Firstly, the emphasis is on active interaction between law enforcement and Internet providers, the recommended guidelines for which have been developed in 2008 by the Council of Europe and the International Project to Combat Cybercrime. The developed guidelines were very successful, as a result of which, in addition to their application at the level of various countries (Ukraine, Romania, France, Georgia, India) (Anderson, Barton, Bölme, Clayton, Ganán, Grasso, and Vasek 2019). The European Court of Human Rights also referred to these guidelines in a decision in the case of KU. v. Finland, in which it emphasized the need for interaction between law enforcement agencies and providers (KU v. Finland (case No. 2872/02). Secondly, at the Eurozone level, various projects are being created and promoted concerning an effective fight against cybercrime in the field of payment processing. Such training systems include both independent training for law enforcement and various concepts and programs for substantive training of prosecutors and judges. This helps train judges and prosecutors to use electronic evidence effectively. On the other hand, the approach promotes a comprehensive assessment of electronic evidence, which forms the basis of cybercrime evidence tools (Urban, Kniazhev, Maydykov, Yemelyanova, 2019).

The issue of cybercrime is also relevant for developing and least developed countries. In the Russian Federation, as of 2019, financial companies were victims of theft of funds from their or client accounts in 76% of cases. At the same time, within the framework of representatives of big business, victims faced direct financial losses in 29% of cases and financial losses of their customers in 23% of cases. At the same time, in the framework of small and medium-sized businesses, such indicators were 15% and 12%, respectively (Positive Technologies and Microsoft 2019). At the same time, in Kazakhstan in 2017, the concept of cybersecurity "Cybershield Kazakhstan" has been established. This concept focuses specifically on measures to prevent cybercrime. In particular, regarding preventive measures, two main methods are indicated. Firstly, ensuring the security of the software against the penetration of malware by cybercriminals. Secondly, the leveling of the human factor, that is, counteracting the consumer's desire to save by installing unlicensed software, as a result of which such a consumer often becomes a victim of a criminal.National educational programs for PC users at no cost are also among preventive measures (Ospanov *et al*. 2019).

Regarding the differences in the issue of cybersecurity and the use of cyberspace in general in highly developed and least developed countries, two key points should be noted, one of which is a kind of consequence of the other. Firstly, there is a significant digital gap in the potentials of either group of states, the possibility or impossibility of wide distribution of cyberspace. Namely, the least developed countries lack the modern means of communication, including broadband Internet and digital trading platforms. Secondly, high-tech states (by analogy with enterprises) widely use information technologies in all fields of activity, in contrast to the least developed states. For example, e-government, distance learning system and more. Studying Bangladesh's experience, problems with countering cybercrime in the field of digital banking are noted.Traditionally, in this country, cybercriminals hack into user accounts and withdraw money from them. In addition, in Bangladesh, cybercriminals use digital banking to transfer illegally received money to other countries; digital banking is also used to pay dealers, human trafficking, etc. As a means of preventing and combating cybercrime in the field of payment processing, this country has developed software to prevent and combat cybercrime. There is as well an interaction of the police, banking, financial and other institutions in the process of investigating committed cybercrimes in the field of payment processing (Mandal 2019; Kathuria, Grover, Perego, Mattoo, and Banerjee 2019).

Let us consider cybercrime in the field of payment processing in Zimbabwe. The key problems in this country are hacking, identity theft of customers of banking and financial institutions, card fraud, the use of malware and phishing. With regard to countermeasures, in Zimbabwe, educational programs, strict IT security, and the improvement of technologies for countering cybercrime are recognized as the most effective in countering cybercrime.In addition, such measures as access control measures, the installation of biometric security, the use of smart cards, and the separation of the most important banking applications from the Internet are recognized as expected by the state (Mugari *et al*. 2016).

Turning to the specifics of committing cybercrime in the field of payment processing, a typical scheme for committing such a cybercrime should be highlighted. A typical scheme of cybercrime against a credit or other financial institution, that is, cyberattacks on public relations in the field of payment processing, as a rule, looks as follows. First of all, the mass mailing of letters initially containing malicious programs to the addresses of credit or financial organizations is carried out. In the event that an employee of one of such companies inadvertently opens such a letter, such programs are automatically installed on the PC Most often, studies show that such a program is a key tool from the Cobalt Strike set - the Beacon component - thanks to which an attacker gains remote access to an affected PC The criminal is trying to establish access to the network domain controller, including through the use of various kinds of special tools and malicious programs, the purpose of which is to obtain administrator passwords. After gaining access to the domain controller and administrator passwords, the attacker searches for computers and networks of interest to him/her, primarily interested in computers from which one can access the subnet that controls, for example, ATMs, payment card processing segments.In the first case, in the affected ATMs, the software is installed that provides the ability to remotely control such an ATM, including the issuance of money on a command sent by an attacker. At the same time, the accomplices of the offender are involved, who, being at the agreed time next to the ATM, receive money issued on such a command. As a general rule, after such an operation, the software is removed from the ATM. In the case of the processing of payment cards, accomplices are also involved who, after committing defeat to the processing segments, draw up payment cards of the attacked organization for straw persons, in fact, attackers get access to the cards.At the same time, after replenishing the balance of such cards, accomplices must cash them out. If, for example, access as a result of a cyberattack was obtained to the computer means of the bank’s payment system or the SWIFT transfer system, then under the control of the offender payments are made to previously stipulated accounts from which funds are subsequently cashed (Kosolapov, Kostromina, and Sivova 2018).

DISCUSSION

In the course of this study, it was found that cybercrime has been a harmful global phenomenon since the beginning of the XXI century, while in recent years it has acquired more sophisticated approaches and types. Cybercrime in the field of payment processing is actively developing (Nagurney 2015). The reason for this is the systematic increase in the number of Internet users, the transfer to cyberspace of many aspects of public life, which causes the criminal interest of attackers (Jain 2020; Kosolapov *et al*. 2018). As a result, in the current level of development of

society, it should be argued that cybercrime in the field of payment processing is becoming a transnational crime. United Nations Convention against Transnational Organized Crime (UNTC) of 2000 and Council of Europe - Convention on Cybercrime (ETS No. 185) of 2001, although they make detailed regulation of types of crimes, including those committed in cyberspace, however, they cannot be absolutely relevant today. Thus, there is a need to sign a new specialized international legal act that would meet the requirements of the time. However, there are problems with the signing of such an agreement, the cause of which can be called the political ambitions of individual states (Gercke 2011; United Nations(UN) 2000). In fact, the signing of international treaties on certain issues is the most faithful and correct way to resolve a specific problem. However, this method is not the only one, since the promotion of international cooperation on countering cybercrime in the field of payment processing is possible in other ways. In particular, through the development of common instructions and recommendations (applicable at the national level) for the contracting parties. Besides, through the approval of educational programs common to the contracting states, on the one hand, for law enforcement officers to investigate and prove the guilt of cybercriminals, on the other hand, for the security sector of financial, banking companies, organizations, as well as ordinary users when making payment transactions. The objectives of such educational programs are measures to prevent cases of impending cybercrime (mainly for security sectors and users).In addition, the task is set to counter already committed cybercrimes. Namely, their effective investigation through the effective use of electronic evidence, judicial proof of the guilt of specific individuals, as well as a mechanism for compensation for losses caused by a cybercrime (Anderson *et al*. 2019, Boin *et al*. 2019, Internet Research Institute 2019; Yakimova and Narutto 2016).

Another area of combating cybercrime is the prevention of legalization (laundering) of proceeds from these crimes (Chernov 2016).

At the same time, given the possible difficulties in the investigation of cybercrime (due to the high level of its latency), special attention should be paid and measures should be taken to prioritize the training of personnel in the security sector of companies, organizations of the banking and financial sectors in line with the effectiveness of detecting cybercrime. It is also worth paying attention to the development of a mechanism and methods for establishing such cases, the immediate transfer of evidence to law enforcement authorities with the aim to initiate proceedings and prosecute perpetrators.

CONCLUSIONS

The issue of combating cybercrime is relevant for each individual state. The study shows that the issue of preventing and combating cybercrime in the field of payment processing is very relevant due to the prevalence and rapid development of this type of crime. This type of cybercrime is even more dangerous because of the target of the defeat - financial concentrations of both state and local budgets, as well as of individual companies and individuals. Therefore, due to the danger of this type of crime and taking into account the positive and negative world experience, the following list of measures to combat cybercrime in the field of payment processing was offered:

- updating the international contractual base by signing on the basis of the existing concept of a new Convention on the fight against the use of information technology for criminal purposes with the aim of internationally resolving the issue of preventing and combating cybercrime in the field of payment processing;

- intensification of interaction between law enforcement agencies with each other, with supervisory authorities, as well as with Internet providers, with state and non-state research and educational institutions, with banks and other financial institutions, as well as with public organizations. Interaction should be carried out by adopting interdepartmental legal acts regulating such interaction. Interaction with the aim of effectively fulfilling the assigned tasks with the rejection of duplication of powers of the authorities, establishing the process of exchange of information regarding cases of preparation or commission of cybercrimes and a number of other events. The issues of such interaction are the study of cybercrime implementation specifics, prerequisites and features of the concealment of criminal acts. In addition, in accordance with the experience of European countries, law enforcement agencies, as well as supervisory authorities, should interact without competition between them or race for performance indicators of a separate law

enforcement agency. At the same time, interaction should occur based on the principles of legality, mutual complementation, at the same time, the independence of each individual body;

- Department of Education (ED), Department of Internal Affairs(DIA), as well as special services should create joint specialized educational programs (based at legal, scientific and educational institutions) for training and professional development of specialists in the fight against cybercrime related to payment processing. European states have separate training of prosecutors (for the purpose of effective prosecution of cybercriminals in the courts) and judges (with the aim of effectively and objectively evaluating the provided evidence and its use or non-use for imputation).This approach is correct because of the need for narrowly focused and specialized training, since the specifics of the activities of a police officer, prosecutor and judge are somewhat different from each other;

- creation by educational departments of educational programs for Internet users in order to ensure their Internet literacy. The example of the Republic of Kazakhstan indicates the need for state financing of such programs, since protecting users during various payment transactions is a state interest in view of the principle that the safety of an individual leads to the safety of a state as a whole.

- the creation of authorities specialized in the detection and prosecution of cybercrime within the Ministry of Internal Affairs and special services, both through retraining of employees and through the recruitment of new employees;

- involving in the process of preventing cybercrime both commercial and non-commercial organizations in the field of information technology in order to create effective licensed software for detecting the facts of the preparation and commission of cybercrime in the field of payment processing; payment for the acquisition and use of such software will go directly to such organizations. In addition, the interest of organizations is also manifested in the very fact of the need to prevent and combat cybercrime in the field of payment processing, in order to avoid their victimization in the future;

- coercion of companies and organizations to follow and apply international standards to counter cyberattacks through regular monitoring by government oversight bodies;

- regular internal audits conducted by companies and organizations to prevent, counteract cyberattacks and notify competent internal affairs bodies;

- active international cooperation of states on the issues of prevention and combating cybercrime in the field of payment processing both at the level of signing general agreements, adoption of common concepts, and at the level of conducting general control and research on the problem of cybercrime.

REFERENCES

Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., &Vasek, M. (2019). Measuring the changing cost of cybercrime. In *The 2019 Workshop on the Economics of Information Security*. Boston, US.

Boin, A., Bynander, F., Jann, W., Schulze-Gabrechten, L., Lodge, M., Lægreid, P., ... &Ryssdal, A. (2019). Institutional Arrangements within the Field of Societal Security and Crisis Management in Germany, Norway, Sweden, the Netherlands and the UK 2018. In *Societal Security and Crisis Management* (pp. 361-387). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-92303-1_19

Center for Strategic and International Studies (2018). Economic Impact of Cybercrime. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime

Center for Strategic and International Studies (2020). Cybersecurity and the Problem of Interoperability. Retrieved from https://www.csis.org/analysis/cybersecurity-and-problem-interoperability

Chernov, S.B. (2016). Money laundering as a threat to the security of the Russian economy. *University Bulletin (State University of Management), 2*, 98-105.

Chernov, S.B. (2019). The policy of combating the financing of terrorism: definition and threats in the conditions of artificial intelligence market development. *Economic Sciences, 7,* 81 – 88.

DLA Piper's Cybersecurity and Data Protection Team (2020). DLA Piper GDPR data breach survey.

Gercke, M. (2011). 10 years Convention on Cybercrime: Achievements and Failures of the Council of Europe's Instrument in the Fight against Internet-related Crimes. *Computer law review international, 5,* 142-149. https://doi.org/10.9785/ovs-cri-2011-142

Global Cybersecurity Index (GCI) 2018 (2018). Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

International Telecommunication Union (2019). Most of the offline population lives in least developed countries. Retrieved from https://itu.foleon.com/itu/measuring-digital-development/offline-population/

Internet Research Institute (2019) *Analysis of the United States' cybersecurity strategic planning documents*. Moscow.

Jain, A. (2020). Cyber Crime. *National Journal of Cyber Security Law, 2*(2).

Kathuria, S., Grover, A., Perego, V. M. E., Mattoo, A., & Banerjee, P. (2019). *Unleashing e-commerce for South Asian integration*. The World Bank. https://doi.org/10.1596/978-1-4648-1519-5

Klochkova, E., Tyurina, Y., Chernov, S., &Glembotskaya, G. (2019). Methods for evaluating economy information potential. *RevistaEspacios*, *40*(38).

Korobeyev, A. I., Dremlyuga, R. I. &Kuchina, Y. O. (2019). Cybercrime in the Russian Federation: criminological analysis. *All-Russian Criminological Journal, 13*(3). https://doi.org/10.17150/2500-4255.2019.13(3).416-425

Kosolapov, Y. V., Kostromina, E. A. &Sivova, A. A. (2018). Cybercrime in the financial services industry. *Economics and Law, 118*, 25-29.

Lakomov, A. S. (2019). Cybercrime: current trends. *Academic thought, 2*(7), 1-17.

Leukfeldt, E. R. (2014). Cybercrime and social ties. *Trends in organized crime, 17*(4), 231-249. https://doi.org/10.1007/s12117-014-9229-5

Mandal, A. (2019). Mobile Banking–A Bangladesh Perspective.

Mugari, I., Gona, S., Maunga, M., &Chiyambiro, R. (2016). Cybercrime-the emerging threat to the financial services sector in Zimbabwe. *Mediterranean Journal of Social Sciences*, *7*(3 S1), 135. https://doi.org/10.5901/mjss.2016.v7n3s1p135

Nagurney, A. (2015). A multiproduct network economic model of cybercrime in financial services. *Service Science, 7*(1), 70-81. https://doi.org/10.1287/serv.2015.0095

Nazmeyeva, L. R. (2020). The digital transformation of the economy: the impact on crime and the issues of its prevention. *Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia, 11*(1(39)).

Orji, U. J. (2019). A Review of the ECOWAS Cybercrime Directive. *Computer Law Review International, 20*(2): 40-53. https://doi.org/10.9785/cri-2019-200204

Ospanov, B. I., Nurusheva, A. M. &Nurushev, M. Zh. (2019). About new joint methods of protection against cyberattacks in Kazakhstan. *Bulletin of the Orenburg Scientific Center of the Ural Branch of the Russian Academy of Sciences, 1*, 28-34.

Positive Technologies & Microsoft (2019). Assessment of cyber security of Russian business. Retrieved from https://3er1viui9wo30pkxh1v2nh4w-wpengine.netdna-ssl.com/wp-content/uploads/prod/sites/46/2019/12/Microsoft-%D0%B8-Positive-Technologies_Final.pdf

Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. *International Journal of Current Research & Academic Review, 2*(2), 173-178.

United Nations (2000). Convention against transnational organized crime. *General Assembly Resolution 55/25*.

Urban, V., Kniazhev, V., Maydykov, A., &Yemelyanova, E. (2019). Implementation of the law enforcement function of the state in the field of countering crimes committed using the internet. In *Big Data-driven World: Legislation Issues and Control Technologies* (pp. 113-120). Springer, Cham. https://doi.org/10.1007/978-3-030-01358-5_11

WeulenKranenbarg, M., Holt, T. J., & Van Gelder, J. L. (2019). Off ending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*, *40*(1), 40-55. https://doi.org/10.1080/01639625.2017.1411030

World Economic Forum (2019). Regional Risks for Doing Business. Insight Report. https://doi.org/10.1016/S1361-3723(19)30016-8

Yakimova, E. M. &Narutto, S. V. (2016). International cooperation in the fight against cybercrime. *All-Russian journal of criminology, 10*(2): 45-66.

Received on 26-10-2020 Accepted on 28-11-2020 Published on 26-12-2020

DOI: https://doi.org/10.6000/1929-4409.2020.09.237