

# CRIMINAL LAW MEASURES OF ENSURING THE SECURITY OF THE CRYPTO SPHERE

*Oleg A. Stepanov, Denis A. Pechegin*

*The Institute of legislation and comparative law under the government of the Russian Federation, Department of criminal, criminal procedural law; judicial system*

**Abstract:** In the first issue of the Bratislava Law Review magazine for 2018, our article addressed the problem of legal regulation of relations related to the crypto sphere “Failure to repatriate funds in foreign currency from abroad and modern issues of currency regulation” was published. In December 2017, Bitcoin predicted the cost of \$ 40 – \$ 100 thousand. However, in 2018, the situation changed-the Bitcoin exchange rate began to lose from \$ 0.5 to \$ 1 thousand per day, and its market capitalization fell to \$ 70 billion<sup>1</sup>. The crisis of the crypto market has affected not only the capitalization of cryptocurrencies, but also the issues of legal regulation of relations associated with its use. Currently, only three countries – Sweden, the Netherlands and Japan – recognize cryptocurrency as a legal means of payment. In Spain, the cryptocurrency is classified as an electronic means of payment only in relation to the gaming business. The legislation of Germany, as well as Finland, allows to classify cryptocurrencies as financial instruments. In China, Singapore and Norway cryptocurrency is considered as a financial asset in the US – as property, i.e. developed countries are in no hurry to equate cryptocurrency to means of payment. In Russia, the use of cryptocurrencies is not regulated by any rules, but there is no legislation prohibiting the circulation of cryptocurrencies as means of payment. At the same time, the draft bill “On digital financial assets”, designed to regulate financial relations in the crypto sphere, completely excludes the issues of mining and circulation of existing crypto-currencies. However, new electronic entities carry certain risks associated with their turnover. In this regard, many States seek to develop mechanisms to ensure the security of actions in the new crypto sphere of legal relations before the direct legalization of cryptocurrencies and other modern electronic entities. The purpose of the article is to analyze the approaches related to the security of the crypto sphere in modern society by criminal law measures taking into account foreign experience.

**Keywords:** cryptocurrency, cybersecurity, cryptosphere development, FATE, criminal law measures, Germany

## 1 INTRODUCTION

According to the estimates of the European Bank (ECB)<sup>2</sup> and a number of national banks, including the Central Bank of Russia, the circulation of private cryptocurrencies, which are not secured and

<sup>1</sup> SAVKIN, Alexey. Cryptomarket: game end, what next // Money. Addition to «КоммерсантЪ». 19. 12. 2018. P. 26 – 27. Available at: <<https://www.kommersant.ru/doc/3828779>>.

<sup>2</sup> Available at: <<https://assets.kpmg.com/content/dam/kpmg/ru/pdf/2017/11/ru-ru-cryptocurrency-legislative-regulation-worldwide-november-2017-upd.pdf>> (A review of the legislative regulation of the cryptocurrency in some States); Virtual Currency Schemes. ECB Report. October 2012. P. 13. Available at: <<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>>.

guaranteed by any state, carries high risks for both consumers and investors, and operations with cryptocurrencies can be used to launder proceeds of crime.<sup>3</sup>

It is important to note that in recent years, not only in Russia but also in other countries are paying more attention to the topic of ensuring the security of the crypto sphere. Thus, on November 12, 2018, the President of France E. macron spoke at the UNESCO Forum on Internet governance with the so-called Paris call for trust and security in cyberspace, which proposes to develop common principles for ensuring security in cyberspace. The Declaration was supported by 51 States, 50 international and regional organizations, more than 170 private companies and corporations. Among them are such leading multinational corporations as Microsoft, Facebook, IBM, Siemens, Daimler Group, Dell Technologies, Hitachi, Panasonic, Airbus and others. At the same time, the entities supporting the Paris appeal undertake, in particular, to work to strengthen law enforcement measures and resistance to malicious actions in the online space, as well as to improve the security of digital products and services, universal "cyber-hygiene".<sup>4</sup>

In addition, it should be noted that in July 2018, the G20 member countries signed an agreement, according to which in 2018 a standard for combating money laundering (AML) in the cryptocurrency sphere was to be developed.<sup>5</sup> At the same time, FATF (The group for the development of financial measures to combat money laundering<sup>6</sup>) expressed its readiness to present AML standards for cryptocurrencies<sup>7</sup>, related to countering money laundering and financing of terrorism for the cryptocurrency market only in June 2019.

Although the details of these rules are not yet known to us, in 2019 the existing FATF rules should be applied to regulate the digital asset market in the member States of the organization, whose governments are required to implement new standards in their legislation before the visit of the FATF assessment Commission in March 2019. In this regard, for example, the government of Japan has already announced its intention to establish mandatory supranational rules for the regulation of crypto-exchanges no later than 2019.<sup>8</sup>

Independently deciding to what extent to regulate the activities of cryptocurrency companies in connection with their obligations, FATF member countries are called upon to give legal status to such standards in each jurisdiction.

In Slovakia, the supervision of virtual currencies is not carried out, although the need for this is obvious in view of the development of financial and economic relations in the European Union<sup>9</sup>.

<sup>3</sup> Forgotten mining: why business is dissatisfied with the law on crypto regulation. Available at: <<https://www.rbc.ru/finances/28/11/2018/5bfd22239a794758092fe326>>.

<sup>4</sup> Available at: <[https://ria.ru/20181112/1532642131.html?referrer\\_block=index\\_archive\\_10](https://ria.ru/20181112/1532642131.html?referrer_block=index_archive_10)>.

<sup>5</sup> G20 will develop standards for combating money laundering with the use of cryptocurrencies. Available at: <<https://forklog.com/g20-razrabotaet-standarty-protivodejstviya-otmyvaniyu-dohodov-s-pomoshhyu-kriptovalyut/>>; <<https://complyadvantage.com/blog/aml-compliance-trends-2019/>>.

<sup>6</sup> FATF currently consists of 37 jurisdictions and two regional organizations representing most of the major financial centers in all parts of the globe. Available at: <<http://www.fedsfm.ru/activity/fatf>>.

<sup>7</sup> Available at: <<https://www.financemagnates.com/cryptocurrency/regulation/financial-action-task-force-to-issue-its-crypto-guidelines-by-mid-2019/>>.

<sup>8</sup> FATF will develop common rules for Bitcoin-exchange in the whole world. Available at: <<https://forklog.com/fatf-razrabotaet-edinye-pravila-dlya-bitkoin-birzh-vo-vsem-mire/>>.

<sup>9</sup> BELOMYTTSEVA, Olga. On the position of the EU countries in relation to the issue and circulation of virtual currencies // Problems of Accounting and Finance. 2015. № 1. P. 26 – 30.

## 2 FUNDAMENTAL PRINCIPLES OF ENSURING THE SECURITY OF THE CRYPTO SPHERE

Legal insecurity of the crypto-sphere, exposed to criminogenic risks, makes it socially dangerous. Moreover, the criminogenic risks in this case is understood as the probability (possibility) of the occurrence of criminogenic consequences caused by the uncertainty of the parameters of social and legal regulation of social relations. These are risks that have a positive impact on the formation of a criminal plan, the purpose of the crime and are associated with the creation of favorable conditions for achieving a criminal result.

It is important to note that currently the creation of such conditions is hampered by the lack of legal capacity of law enforcement agencies to prevent and respond to criminal manifestations in this area, in particular related to the payment of terrorist activities “virtual currency”, the use of which implies the anonymity of transactions and users, fast speed of transactions.

Meanwhile, the practical implementation of measures to neutralize the criminal threats associated with the use of cryptocurrency involves the implementation of appropriate conditions for the implementation of legal regulation of the development of the crypto sphere. The implementation of such conditions is due to the need for a consistent criminal law policy, which should be based on the following basic principles:

- the principle of justice, according to which measures taken against a particular person about his actions related to the use of cryptocurrency should be based on the possibility of balancing the interests of the individual, society and the state;
- the principle of adequate response to any criminal manifestation, on the basis of which the offender is necessarily subjected to specific measures of state influence, regardless of his official, professional, property status, and law enforcement agencies are designed to ensure the neutralization of negative consequences in the context of digitalization of public practice. At the same time, law enforcement officers should acquire new skills in the use of information technologies (cryptodetective skills) related to the structuring of large amounts of information, its correct search, analysis and selection, i.e. they should move from “repeaters” to the category of “communicators” of legal information designed to quickly navigate in its flow, master the logic of its search. It is on this that the success of their investigation of crimes will depend to a large extent.

According to experts, almost every day on the Internet there are financial pyramids based on cryptocurrency investments, because the blockchain technology is convenient for building such pyramids – eliminates the need to make payments manually and maintain any databases to someone who, using smart contracts, controls the accession to the pyramid.<sup>10</sup>

There are no legislative methods to combat this phenomenon. There is no crime, there is no evidence, there is no possibility to find the organizer. In this regard, the issue of improving criminal legislation is becoming more urgent.

The system of means providing effective criminal and legal impact on new social relations, as such, is a combination of interrelated legal, socio – economic and psychological elements that determine the volitional behavior of participants in crypto-relations. Therefore, we can talk about a specific set of means of regulating social relations using different approaches.

---

<sup>10</sup> «Коммерсантъ». 21. 12. 2018. № 236.

In this regard, it is very important to analyze the General and special rules for the construction of crimes<sup>11</sup> on qualifying and privileged grounds<sup>12</sup>, as well as the allocation of rules for the construction of qualified compositions<sup>13</sup>, rules for the construction of sanctions of criminal law<sup>14</sup>.

According to V. K. Andrianov analysis of the structural patterns it is logical to carry out the private patterns, which expresses the internal structure of a separate criminal legal phenomena, to more General, characterizing the internal structure of the criminal law system.<sup>15</sup>

### 3 GERMANY – A VIEW ON THE DEVELOPMENT OF CRIMINAL LAW MEASURES TO RESPOND TO NEW TECHNOLOGICAL CHALLENGES

At the same time, in our opinion, the experience of Germany is interesting, where it is considered inappropriate to introduce new crimes in the criminal code of the country, including in response to the development of the crypto sphere.

Comprehensive legal regulation of relations arising in connection with the development of the digital economy involves the establishment of the grounds and conditions for bringing persons to responsibility for illegal actions in the new crypto sphere of legal relations, including criminal. At the same time, this issue is most acute in connection with the emergence and evolution of crypto – currencies-digital entities that erase any boundaries, allowing you to move away from accounting for income, paying taxes, controlling financial flows, and so on. The latter is related to the risks and threats posed by this “new money”<sup>16</sup>. After all, unlike the use of digital technologies (i.e. the appropriate software) for criminal purposes, where a certain qualification of the attacker is required, almost everyone can use the cryptocurrency to commit illegal actions.

Recall that since 2013, the government of Germany began to recognize Bitcoin as a digital currency, indicating that such currency does not apply to electronic money or to the so-called “functional” currency (including foreign). In the future, virtual currencies in Germany were recognized as a financial instrument (2017), and in the banking legislation of Germany they were recognized as private funds and specific units of financial accounting.

However, according to experts, the new “money” carry an excessive number of risks that can have a negative impact not only on the welfare of specific citizens, but also the national economy, and “anonymity”<sup>17</sup> and the lack of control of national authorities attracts the attention of crime

<sup>11</sup> IVANCHIN, Artem. Conceptual bases of designing of structure of a crime: dissertation, doctor of law. Yaroslavl, 2014. 462 p.

<sup>12</sup> LESNIEWSKI-KOSTAREVA, Tatiana. Differentiation of criminal responsibility. Theory and legislative practice. Moscow, 2000. P. 257 – 271.

<sup>13</sup> KRUGLIKOV, Lev. Problems of the theory of criminal law: selected articles, 2000 – 2009. Yaroslavl, 2010. 591 p.

<sup>14</sup> GUSTOVA, Ella. Construction of sanctions in the criminal law of the Russian Federation: theoretical aspect: dissertation, PhD. Voronezh, 2015. 204 p.

<sup>15</sup> ANDRIANOV, Vladimir. Structural regularities of criminal law: concept, types, correlation of concepts // Journal of Russian Law. 2018. № 10. P. 91 – 100.

<sup>16</sup> PECHEGIN, Denis. Cryptorisks // Russian Journal of Legal Studies. № 3. 2017. P. 153.

<sup>17</sup> At its core, cryptocurrency is anonymous, although there already exist programs that allow to de-anonymize the ultimate owner of a particular cryptocurrency or cryptoasset.

in the legalization (laundering) of proceeds obtained by criminal means to modern money surrogates<sup>18</sup>.

Thus, the German police are increasingly faced with criminals and entire groups that commit crimes on the Internet using high-tech equipment. The Central task of the German law enforcement agencies in this area is to prevent the Commission of illegal actions. The response to the development of crime in the economy 2.0, 3.0, 4.0 should be adequate. Forensic techniques and techniques should also meet levels 2.0, 3.0 and above. This is done by the departments for combating cybercrime and digital investigations of criminal investigation of a particular land of Germany.

However, the investigation against cybercriminals is further complicated by some factors. For example, cybercriminals are increasingly operating from Darknet – the so-called “dark” Internet. In this area of the Internet, criminals can use special encryption tools and technologies to maximize the anonymity of their traffic.

Another factor that complicates the possibility of combating cybercrime is that most crimes in this area are not local. This implies that the public authorities of different States should cooperate more closely at the international level. However, such cooperation at the international level is complicated by the fact that the common principles of interaction between countries related to the understanding of the nature of modern digital entities have not yet been developed, which is largely due to national differences in the sphere of legislative regulation of various issues arising in the field of innovation and monetary relations.

Meanwhile, all criminal actions in the virtual world are somehow connected, as representatives of the German legal doctrine believe<sup>19</sup>, with the interface of entering the real world. This is the key to the success of the investigation by the relevant departments of the criminal investigation Department of a particular state of Germany<sup>20</sup>.

Cybercrime in Germany includes all crimes against the Internet, additional data networks of information systems or their data in accordance with the national definition. Cybercrime also includes crimes committed with the help of information technology.<sup>21</sup>

The German law enforcement officer thus proceeds from a broad understanding of cybercrime and includes, among other things, acts committed by means of speech (including the dissemination of pornography and extremist propaganda), as well as invasion of the personal sphere of human life, fraud and computer fraud, software and hardware attacks (including preparation for information

<sup>18</sup> POLASIK, Michal, PIOTROWSKA, Anna, WISNIEWSKI, Tomasz, KOTKOWSKI, Radoslav, LIGHTFOOT, Geoff. Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry, 2014. p. 20 – 21. [online]. Available at: <<https://ssrn.com/abstract=2516754>>; LUTHER, William. Bitcoin and the Future of Digital Payments. 14 p. [online]. Available at: <<https://ssrn.com/abstract=2631314>>; BRYANS, Danton. Bitcoin and Money Laundering: Mining for an Effective Solution // 89 Ind. L.J. 2014. P. 441 – 472. [online]. Available at: <<https://ssrn.com/abstract=2317990>>; etc.

<sup>19</sup> Available at: <<https://www.bitcrime.de/presse-publikationen/pdf/BITCRIME-RegulRep.pdf>>; BRENIG, Christian, ACCORSI, Rafael, MÜLLER, Günter. Economic Analysis of Cryptocurrency Backed Money Laundering // ECIS Completed Research Papers. 2015. Paper 20. [online]. Available at: <[https://aisel.aisnet.org/ecis2015\\_cr/20/](https://aisel.aisnet.org/ecis2015_cr/20/)>; GRZYWOTZ, Johanna, KÖHLER, Olaf, RÜCKERT, Christian. Cybercrime mit Bitcoins – Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention // StV. № 11. 2016. P. 753 – 759 [online]. Available at: <<https://www.bitcrime.de/presse-publikationen/>>.

<sup>20</sup> So, the police of Baden-Württemberg for several years ago introduced a special position of cybercriminality. Particularly skilled professionals serve in the cybercrime and digital investigations division of the criminal investigation Department, as well as in the relevant criminal inspections of the twelve regional police headquarters.

<sup>21</sup> Available at: <[https://lka.polizei-bw.de/wp-content/uploads/sites/14/2017/06/Cybercrime\\_Digitale\\_Spuren.pdf](https://lka.polizei-bw.de/wp-content/uploads/sites/14/2017/06/Cybercrime_Digitale_Spuren.pdf)>; <<https://cyberleninka.ru/article/v/kiber-i-internet-prestupnost-v-germanii-i-rossii-vozmozhnosti-sravnitel'nogo-issledovaniya>>.

theft), forgery of documents by means of a computer, falsification of data essential for proof, and other computer crimes<sup>22</sup>. In other words, this category of crime in German criminal law is basically related to property acts. However, the realities of cybercrime and the scale of the increase in the number of criminal acts in this area are far ahead of the legislator.

The Federal criminal police service of Germany (Bundeskriminalamt) presented the annual report on the state of cybercrime in the country for 2017.<sup>23</sup> This report also included information about crimes related to cryptocurrency. Moreover, many malicious programs today focus on illegally and imperceptibly using the resources of a company or an individual user in order to carry out hidden cryptomining, including the well-known digital currency Bitcoin. And for this today it is not necessary to infect the computer of a particular user, the corresponding scripts that will “exhaust” the energy of your computer can now be embedded in sites and videos (music). Going to a particular resource and clicking “Play” the user automatically allows such a resource to use the computing power of his computer as long as he uses this resource.

The complexity of the qualification of such an act is that such programs often do not violate the integrity of the system itself, but simply load it much more while the user accesses the Internet resource. In other words, as soon as the user closes the site or browser, the corresponding script will stop its execution and will not harm the user’s system. The criminal code of Germany contains a separate crime, provided for in § 303a, which establishes responsibility for illegal deletion, conversion, scrapping, and modifying user data.

However, in order to qualify the case described above under § 303a of the Criminal code of Germany, the corresponding script must penetrate into the affected system and create conditions in this system for constant communication with the corresponding server. In the latter case, such an act falls under the signs of the crime provided for in § 303a of the Criminal code of Germany, since here, most likely, there will be a secret and unauthorized change of user data. At the same time, for such a conclusion, the software of the corresponding computer, in theory, should become a single, in the likeness of blockchain technology, when any change requires the creation of a new block, which will easily identify unauthorized changes in the system. But even without such a structure of the software of a particular user, this case, in General, falls under § 303a of the Criminal code of Germany.

The land court of Kempten (Bavaria), in its decision<sup>24</sup> of 27 July 2017, pointed out that the change in data within the meaning of paragraph 1 § 303a of the Criminal code of Germany occurs as a result of a violation of the functions of data that lead to a change in their information content or indicator. This includes any form of transformation of the contents of the stored data, and it does not matter whether it is an objective improvement. Rather, it is crucial that the state of the system is different from the previous one. At the same time, the user is obliged to take measures to protect their information, for example, to use a firewall that will not allow an ordinary user without special training to access the information system. However, this does not mean that the offender will avoid responsibility in the latter case. In the case of 75% of infected computers, the firewall was turned on

<sup>22</sup> SIEGMUNT, Olga. Cyber and internet crime in the Federal Republic of Germany and the Russian Federation: possibilities for a comparative research // *Legal Science and Law Enforcement Practice*. № 4 (34). 2015. P. 182.

<sup>23</sup> Available at: <<https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017>>.

<sup>24</sup> BGH 1 StR 412/16 – Beschluss vom 27. Juli 2017 (LG Kempten). [online]. Available at: <<https://www.hrr-strafrecht.de/hrr/1/16/1-412-16.php>>.

automatically, whereas in 25% cases, this program has been deactivated. At the same time, malicious software was secretly installed on users computers and had the ability to bypass firewall protection. Therefore, all cases established by the court were correctly qualified under § 303a of the Criminal code of Germany.

On the other hand, modern technologies make it possible to do without changing the relevant data or infecting the computer, which requires independent understanding from the point of view of the description of the criminal act in the doctrine of criminal law and further, respectively, in the criminal law. In particular, the border beyond which criminal liability will be established in case of unauthorized use of the computer resources of the user who visited this or that Internet resource requires a separate understanding<sup>25</sup>. After all, these scripts can be very successfully used by advertisers instead of referring to banners, which sometimes too intrusively offer any product to the user and to a greater extent load the operating system of the user's computer. However, this problem in the science of criminal law in Germany has not been solved.

## 4 CONCLUSION

Analysis of foreign legislation in connection with the problem of determining the order and grounds of liability in the new crypto-sphere of legal relations allows us to distinguish four approaches to changing the criminal law: 1) introduction of specific compositions listed in the Special part, additional provisions related to the crypto-sphere; 2) establishment and definition of new crimes; 3) use of existing crimes to regulate liability in the new crypto-sphere of legal relations; 4) partial or full use of all listed options at the same time.

Attempts to solve this problem in Germany are based on the fact that the German doctrine States cases of crimes committed using digital technologies. But since such acts are often cross-border in nature, this significantly complicates the ability of German law enforcement agencies to obtain timely and full evidence in criminal cases. In addition, there are some difficulties in the qualification of crimes committed with the use of digital technologies, since most of them are German law enforcement officers trying to bring under the existing compositions. However, this approach does not make it possible to conclude unequivocally that the punishment determined by the current norms of the criminal code of Germany really corresponds to the social danger that the crimes committed with the use of digital technologies contain.

It seems that the identified problems can be solved at a qualitative level only if there is an international standard for combating crimes committed with the use of modern digital technologies. As part of the definition of approaches to ensuring the security of the crypto sphere, illegal actions of the individual can rightly be considered as part of the General chain of natural relationships and processes associated with its development. In order to study such actions, it is necessary to identify and analyze the causes of both criminal liability and the adaptation of criminal legislation to the new historical realities not only at the national but also at the international level.

---

<sup>25</sup> KHABRIEVA, Talia. Law Facing the Challenges of Digital Reality // Journal of Russian Law. № 9. 2018. p. 5 – 16; KHABRIEVA, Talia, CHERNOGOR, Nikolay. The Law in the Conditions of Digital Reality // Journal of Russian Law. № 1. 2018. P. 85 – 102.

**Bibliography:**

- ANDRIANOV, V. Structural regularities of criminal law: concept, types, correlation of concepts, *Journal of Russian Law*, 2018, № 10, P. 91 – 100.
- BELOMYTTSEVA, O. On the position of the EU countries in relation to the issue and circulation of virtual currencies, *Problems of Accounting and Finance*, 2015.
- BRENIG, C. – ACCORSI, R. – MÜLLER, G. Economic Analysis of Cryptocurrency Backed Money Laundering, *ECIS Completed Research Papers*, 2015.
- BRYANS, D. Bitcoin and Money Laundering: Mining for an Effective Solution, 89 *Ind. L.J.*, 2014.
- GRZYWOTZ, J. – KÖHLER, O. – RÜCKERT, C. Cybercrime mit Bitcoins – Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention, *StV*, № 11, 2016.
- GUSTOVA, E. Construction of sanctions in the criminal law of the Russian Federation: theoretical aspect: dissertation, PhD, Voronezh, 2015.
- IVANCHIN, A. Conceptual bases of designing of structure of a crime: dissertation, doctor of law, Yaroslavl, 2014.
- KRUGLIKOV, L. Problems of the theory of criminal law: selected articles, 2000 – 2009, Yaroslavl, 2010.
- LESNIEWSKI-KOSTAREVA, T. Differentiation of criminal responsibility, *Theory and legislative practice*, Moscow, 2000.
- LUTHER, W. Bitcoin and the Future of Digital Payments, 2015.
- PECHEGIN, D. Cryptorisks, *Russian Journal of Legal Studies*, № 3, 2017.
- POLASIK, M. – PIOTROWSKA, A. – WISNIEWSKI, T. – KOTKOWSKI, R.
- LIGHTFOOT, G. Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry, 2014.
- SIEGMUNT, O. Cyber and internet crime in the Federal Republic of Germany and the Russian Federation: possibilities for a comparative research, *Legal Science and Law Enforcement Practice*, № 4 (34), 2015.
- STEPANOV, O. – PECHEGIN, D. Failure to repatriate funds in foreign currency from abroad and modern issues of currency regulation, *Bratislava Law Review*, Vol. 2, № 1, 2018.

**Contact information:**

prof. Oleg A. Stepanov, Dr.  
crim5@izak.ru

The Institute of legislation and comparative law under the government of the  
Russian Federation, Department of criminal, criminal procedural law; judicial system  
117218, B. Cheremushkinskaya 34  
Moscow  
The Russian Federation

Denis A. Pechegin, Ph.D.  
crim5@izak.ru

The Institute of legislation and comparative law under the government of the  
Russian Federation, Department of criminal, criminal procedural law; judicial system  
117218, B. Cheremushkinskaya 34  
Moscow  
The Russian Federation