

● **Problematic Aspects of the Efficiency of Rules Providing for Criminal Liability for the Commission of Crimes in the Field of Computer Information.**

Denis A. Garbatovich – PhD in Law, Dean of the Law Faculty of the Chelyabinsk Branch of the Russian Academy of Education University.

The article considers the effectiveness of the criminal law rules providing for responsibility for committing crimes in the field of computer information through analysis of such criteria as: 1) stability of the criminal law rules; 2) problems of the protection of public relations through appropriate criminal law rules; 3) problems with the application of the criminal law rules in question; 4) the problem of understanding and application of the terminology used within this group of norms; 5) the problems of punishment prescribed for the commission of offences in the field of computer information.

Keywords: effectiveness of criminal law rules; offences in the field of computer information.

● **Some Criminal Law Innovations Aimed at Ensuring Economic Security in the context of Scientific and Technical Progress.**

Nodar Sh. Kozaev – PhD in Law, Associate Professor in the Department of Criminal Law at the North Ossetian State University named after K.L. Khetagurov.

The article analyses some of the provisions of the Criminal Code of the Russian Federation introduced in connection with the innovation processes and aimed at protecting the economic security.

Keywords: economic security; fraud; computer info; innovations; registries; insider information.

● **Criminal Liability for Unauthorized Access to Computer Information: General Characteristics and Some Problems of Crime Classification.**

Mikhail M. Lapunin – PhD in Law, Associate Professor in the Department of Criminal Law and Correctional Law at Saratov State Law Academy.

The article provides a criminal law analysis of the elements of the offence under Art. 272 of the RF Criminal Code. Statistical data related to this article and examples of judicial practice are presented. The article reveals the features of the notion of “computer information protected by law”. The article touches upon the disputed questions of crime classification, including approaches to the interpretation of the word “computer-related”, the understanding of the destruction of information under this article, and the interplay of sanctions under Part 1 and Part 2 of Art. 272 of the RF Criminal Code. The article considers the relationship between the illegal access to computer information and other crimes (particularly under articles 158, 167, 159.6, 273, 293 of the RF Criminal Code), and proposes relevant rules for classification, including for multiple offences.

Keywords: computer crime; criminal liability for unauthorized access to computer information.

● **Problems of Establishing a Criminal Law Method to Combat Computer Fraud.**

Tatyana M. Lopatina – Doctor of Laws, Associate Professor, Head of the Department of Constitutional Law Disciplines at Smolensk University for the Humanities.

The article presents the author's point of view on fraud in the field of computer information. A critical analysis is performed in relation to the criminal law characteristics of the elements of a crime under Art. 159-6 of the RF Criminal Code. A comparison is drawn with similar rules in the criminal legislations of states with a high level of computerization. Modern types of computer

fraud are outlined, including cash machines, credit cards, payment instruments, slot machines, and Internet fraud. The classification of mobile phone fraud into subscription, hacking, technical, and procedural fraud is also provided.

Keywords: fraud; computer fraud; new types of computer fraud; Internet fraud.

● **The Objective Aspect of Unauthorised Access to Computer Information under the Criminal Code of the Russian Federation.**

Vladimir G. Stepanov-Egiyants – PhD in Law, Associate Professor in the Department of Criminal Law and Criminology, Deputy Dean of the Law Faculty at Lomonosov Moscow State University. The article discusses the terms used in Art. 272 of the RF Criminal Code. In particular, a review is given of the existing definitions of computer information and such notions as destruction, blocking, modification, and copying of computer information. The author examines the possible consequences of the acts provided for in Art. 272 of the Criminal Code assessing them in terms of criminal law, as well as considers the possibility to classify certain offences as minor.

Keywords: computer crimes; unauthorised access to computer data; computer data; destruction, blocking, modification, or copying of computer data.

● **Errors and Difficulties Arising When Classifying Cybercrimes.**

Sergey A. Filimonov – PhD, Senior Lecturer at the Village of Leningradskaya branch of Kuban State University.

At present, the number of cyber crimes committed in the territory of the Russian Federation, as well as in other countries, has been increasing. In the process of investigation and consideration on the merits of criminal cases in this category, there arise various mistakes relating to the classification of criminal acts. These mistakes should be summarised and avoided in the future. In view of this, there is a need to adopt as soon as possible the resolution “On judicial practice in cases of crimes in the field of computer information” of the Plenum of Supreme Court of the Russian Federation. In order to actually combat cybercrime by law enforcement agencies, there is also a need to develop a system of harmonious interaction between these agencies.

Keywords: cyber crimes; information security; classification errors; means of computer communication; computer systems; destruction of traces of a crime.

● **A Theft Using Computer Equipment or Computer Fraud?**

Vadim V. Khiluta – PhD in Law, Associate Professor, Head of the Department of Criminal Law and Criminology at Yanka Kupala State University of Grodno (Belarus).

The article discusses the issues of criminalising “computer theft” in the Russian and foreign legal doctrine. It analyses the factors to be satisfied for the establishment of such liability and the appropriateness of identifying by legislators essence-related features of “computer fraud”. The author attempts to reveal the essence and content of such an independent method of property crimes as theft using computer technology, and to identify the characteristic features of this type of crime. The author justifies his conclusion that the Criminal Code should impose liability for a “theft of property by modifying the results of automated processing of computer systems data”.

Keywords: theft; fraud; theft using computer technology; computer fraud; modification; manipulation.

● **On Some Technical Aspects of the Classification of Crimes in the Field of High Technologies.**

Aleksey N. Yakovlev – PhD in Law, Associate Professor in the Department of Jurisprudence, Intellectual Property and Forensic Examinations at Bauman Moscow State Technical University; Deputy Head of Computer and Technical Investigations Division at the Investigative Committee of the Russian Federation.

The article discusses the terminology base demanded in the classification of criminal actions according to constituent elements of offences under Art. 272-274 of the RF Criminal Code. The

author outlines the problem of subjective approach by participants in criminal proceedings to the interpretation of key terms and definitions in the field of information technology, within the scope of the criminal law rules in question, and suggests switching to their uniform interpretation by participants in criminal proceedings on the basis of terms and definitions available in the regulations on standardisation and other legal regulations.

Keywords: crimes in the field of computer information; destruction, blocking, modification, and copying of information; malware.

CRIMINAL PROCEDURE

● **On the Reliability of “Electronic Evidence” in Criminal Process.**

Aleksander S. Aleksandrov – Doctor of Laws, Professor of the Department of Criminal Procedure at Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia.

Sergey I. Kuvychkov – Lecturer in the Department of Mathematics, Informatics and Information Technologies at Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia.

The article criticizes the ideas about the alleged inferiority of electronic evidence. The authors demonstrate the typical drawbacks in using electronic evidence. They make suggestions for changes in legislation in order to adapt it to the use of electronic information in the proving process. In the article, there are also recommendations for improving the efficiency of presenting electronic evidence in the court.

Keywords: electronic evidence; criminal procedure; proving process.

● **Procedural Procedure for Organizing and Conducting Searches of Premises Which Houses Computer Equipment (According to Ukrainian Legislation).**

Irina V. Ena – Senior Lecturer in the Department of Criminal Law and Justice at Zaporozhye National University.

The article identifies and analyses the factors behind the complexity of the investigation into the so-called ‘computer crimes’. One, and the most important of which, is the lack within law enforcement agencies of recommendations for investigation of this type of offences, and carrying out investigative actions, in particular, search of premises which houses computer equipment. Search, in this case, is the most informative investigation (search) operation to identify and seize information of evidentiary value, which will make it possible to establish the truth in the case. Without conducting a search, it is impossible to investigate the given specific type of crimes, so at present the law enforcement agencies of Ukraine have the need for specific guidelines for its implementation. The author identifies seven main stages in conducting search of premises, which houses computer equipment, and, based on the analysis of the criminal procedure legislation of Ukraine, highlights specific features of each of those stages.

Keywords: computer; computer equipment; electronic computer; computer system; computer network; investigative (search) action; ruling of the investigative judge; search; protocol.

● **Digital Information in the Criminal Process.**

Nikolay A. Ivanov – PhD in Law, Associate Professor in the Department of Criminal Procedure and Criminalistics at Omsk Law Academy.

The paper discusses the different approaches of scientists to the definition of the concepts of machine-readable or computer information. The author substantiates a more broadening interpretation of the information recorded on machine-readable media, providing his own definition of ‘digital information’ for the purposes of criminal proceedings.

Keywords: criminal process; evidence; digital information.

- **Operational and Search Support of Investigating Crimes in the Sphere of Computer Information.**

Aleksandr A. Kosynkin – PhD in Law, Lecturer in the Department of Criminal Law, Criminalistics and Criminology at the Mordovian State University named after N.P. Ogarev.

The article discusses one of the aspects of investigating crimes in the sphere of computer information – its operational and search support. Attention is drawn to the fact that this support is one of the means that can seriously improve the effectiveness of the investigation of the crimes in question. As for the effectiveness of this tool, it very much depends on how it takes into account specific features of the crime being investigated. In addition, these features are largely due to specifics of virtual reality in which to a large extent crimes of this type are being committed. Special attention is given to the fact that well-organised actions of operational and search support can make it possible for the system of proofs formed by an investigator, to be convincing. As regards convincingness, it is the property of a system of proofs that allows the court to accept it as true to render a sentence on its basis.

Keywords: operational and search support; investigation; crimes in the sphere of computer information; data base; evidence.

- **Some Problems of Investigation of Crimes Committed with the Use of Computer Technology.**

Nikolay A. Podolny – Doctor of Laws, Associate Professor, Head of the Department of Criminal Law, Criminalistics and Criminology of the Law Faculty at the Mordovian State University named after N.P. Ogarev.

The article outlines a range of problems, the solution of which would, in the author's opinion, improve the efficiency in investigating crimes committed with the use of computer technology. The major one of these problems, as the author sees it, is the problem of the use of operational and investigative information in the course of the investigation. Therefore, the interaction between the investigator and bodies carrying out operational and search activities is considered. In this connection, attention is drawn to the status of the employee of a body carrying out operational and search activities. Other problems are also analysed, including the problem of overcoming obstruction to investigation; and the problem of persuasiveness of the collected evidence relevant to the case.

Keywords: crime; computer technology; investigation; overcoming obstruction of investigation.

- **Using Electronic (Computer) Documents as Documents of Evidence and Documents of Written Evidence in Procedural Relations.**

Aleksandr V. Tkachev – PhD in Law, Associate Professor in the Department of Criminalistics at Lomonosov Moscow State University.

The article deals with the question of the application of electronic (computer) documents in various types of domestic proceedings: criminal, civil, arbitration. It reviews the ways in which the new type of document is incorporated in procedural relations, and discusses the differences in the use of concepts "document of evidence" and "document of written evidence" when introducing computer documents in procedural relations. Reasons are given for the necessity of a closer relationship between procedural and substantive legal regimes of electronic documents. Proposals to improve Art. 84 of the RF Code of Criminal Procedure are also offered.

Keywords: electronic (computer) documents; evidence; document; written evidence; physical document medium; criminal proceedings; civil proceedings; arbitration proceedings; electronic data medium.

- **Problems of Regulating the Procedure for Conducting Investigative Actions Involving Seizure of Electronic Storage Media.**

Aleksandr V. Shigurov – PhD in Law, Associate Professor in the Department of Criminal Law, Criminalistics and Criminology of the Law Faculty at the Mordovian State University named after N.P. Ogarev.

The article examines the problems of procedural procedure for investigative actions involving seizure of electronic storage media. It analyses the strengths and weaknesses of the innovations introduced into the RF Code of Criminal Procedure by Federal Law № 143-FZ of July 28, 2012. The author justifies the need to specify in law a specific time period to issue copies of electronic storage media, including in the course of inspection, as well as establishing a uniform procedure for obtaining certified copies of seized documents, regardless of their form (electronic or written).

Keywords: criminal proceedings; seizure; search; electronic storage media; copying.

CRIMINOLOGY

● **Problems of Countering Cybercrime in Ukraine.**

Vladimir A. Golubev – PhD in Law, Associate Professor, Director of Computer Crime Research Centre, Zaporozhye, Ukraine.

The paper is focused on the problems of countering cybercrime. On the one hand, the Internet has allowed to commit traditional crimes in more efficient and less risky way, on the other hand – it has generated new, unknown yet types of publicly dangerous encroachments, an aggregate and system of which is expressed in such a negative social phenomenon as Internet criminality. In the new rapidly changing realities of Ukraine, a systems and consistent research of Internet criminality is needed both on the whole and of the most widespread types of it, as well as the development of effective measures to fight and prevent crimes in the Global network.

Keywords: cybercrime; Internet; Ukraine; Internet crime; countering; cyber attacks.

● **On the Adequacy of Criminal Law Rules for the Protection of Public Relations in the Field of Information.**

Tatyana P. Kesareeva – PhD in Law, Associate Professor, Prosecutor in the Organisation and Control Division at the Public Prosecutor's Office of the Moscow Region.

The article, through the prism of provisions on information security, analyses the criminal rules protecting public relations in the field of information. The author comes to the conclusion that the provisions of the current criminal legislation are not adequate to protect the mass consciousness of society and the consciousness of the individual from the effects of harmful information.

Keywords: criminal law rules; crime; relations in the field of information; information security; harmful information.

● **Cybercrime: Forecasts and Problems of Fighting.**

Vitaly A. Nomokonov – Doctor of Laws, Professor in the Department of Criminal Law and Criminology at the Far Eastern Federal University.

Tatyana L. Tropina – PhD in Law, Senior Researcher at the Max-Planck Institute for Foreign and International Criminal Law (Freiburg, Germany).

Crime in cyberspace is one of the most challenging problems that international community has been facing during the last decades due to the development and growth of information and communication technologies. The article analyses phenomenological aspects of crime in the global information networks, discusses the issues of the cybercrime definition, types of crimes in cyberspace, cybercrime development and recent trends. The paper also discusses the problems in fighting cybercrime.

Keywords: cybercrime; computer crime.

- **The Internet in the Mechanism of Criminological Determination.**

Aleksandr A. Smirnov – PhD in Law, Higher Doctorate Candidate at the All-Russian Research Institute of the Ministry of Internal Affairs of the Russian Federation.

The article focuses on studying the role and significance of the Internet in the mechanism of determination of criminal behavior. It substantiates the thesis about that the Internet, as the important element of modern social environment, makes essential impact on society, which is of ambivalent nature. Crime determination is identified as one of the major negative consequences of the Internet's social influence. Traditional sociological and criminological concepts on the role of mass media in this process are quite applicable to the Internet, but not adequate, as they do not consider the specifics of the Internet. The article examines the main views of Russian researchers concerning the Internet's role in determination of criminal behavior, and puts forward a number of the author's hypotheses. Special attention is paid to the victimological aspects related to the behavior of victims of crime in cyberspace.

Keywords: determination; criminal behavior; Internet; social networks; virtual communities.

CRIMINALISTICS

- **On the Recognition of Forensic Examination of Electronic Data Carriers as a New Branch of Forensic Technique.**

Konstantin E. Dyomin – PhD in Law, Associate Professor in the Department of Weapons and Trasology at the Moscow University of the Ministry of Internal Affairs of Russia.

The article looks at the justification of identifying the examination of electronic data carriers as a new branch of forensic technique. The author's definition of this branch is given; its system, subject and purposes are identified.

Keywords: information and telecommunication system; computer crimes; criminalistics technique; radio-electronic device; forensic computer technical expert examination; electronic data carriers.

- **Cybercrime: A Forensic Aspect of the Problem.**

Evgeny P. Ischenko – Doctor of Laws, Professor, Head of the Department of Criminalistics at Kutafin Moscow State Law University (MSLA).

The article looks at such complex phenomena as cyberspace, the global Internet and cybercrime, providing author's own concepts of them and their most characteristic features. Some forensic approaches to the detection and investigation of modern cybercrimes are also revealed.

Keywords: cybercrime; information technology; Internet; cyberspace.

- **Problems of Establishing the Perpetrator of Illegal Access to Computerised Bank Information.**

Valery N. Karagodin – Doctor of Laws, Professor, Honoured Lawyer of Russia, Deputy Director of the Institute for Professional Development of the Investigative Committee of the Russian Federation / Head of the Yekaterinburg branch.

Kirill V. Kostomarov – PhD in Law, Assistant Professor in the Department of Criminal Law Disciplines at the Ural Institute – Branch of the Russian Presidential Academy of National Economy and Public Administration.

The article deals with the problems of establishing perpetrators of illegal access to computerised bank information in different situations. The major difficulties of the investigation are conditioned by the specificity of surrounding circumstances and methods of committing such crimes. The situation around such violation is normally characterized by the

increased technical protection of banks' information systems through applying special modes of access for strictly defined categories of users. These circumstances require a more extensive and complete preparation by perpetrators of illegal access to overcome the protective barriers. The main goal of most crimes of this kind is to gain material benefit. In this regard, the methods of making such attacks include operations to misappropriate funds or to sell illegally obtained information. The content of the methods of crime under analysis varies depending on whether the perpetrators are employees of the bank itself (internal subjects) or not (external subjects). All this causes a specific mechanism of formation of traces, which certainly should be taken into account in the course of pre-trial criminal proceedings. The article analyses the typical problems characterized by the deficiency of data on perpetrators of crimes related to illegal access to computerised bank information and offers recommendations for their resolution. Unlawful access to computerised bank information is often only an element of different techniques to steal bank funds.

Keywords: computer information; establishment of the perpetrator; internal subject; external subject; direct access; remote access; problematic situations; banks.

● **Problems of Search and Recording of Information of a Terrorist and Extremist Nature in the Internet.**

Vladlen V. Kardanov – PhD Student at Kaliningrad Border Guard Institute of the Federal Security Service of the Russian Federation.

The article outlines the main problems associated with finding and recording of information of an extremist nature in the Internet. Possible solutions to these problems are suggested. Examples of practical actions for the implementation of certain operational search measures are also provided.

Keywords: information countermeasures; information recording problems; extremism; terrorism; operational search activities; the Internet.

● **On the Application of Legal Psychology in the Fight against Cybercrime.**

Aleksandr N. Kosenkov – Master of Law (Chernigov, Ukraine).

The article attempts to define the key areas of using legal psychology in the fight against cybercrime. An overview of the applications of legal psychology in combating cybercrime in general and within individual criminal disciplines (such as criminal law, criminology, criminalistics, and criminal executive (correctional) law) is provided. The author addresses some problem points of the fight against cybercrime, which legal psychology can contribute to their solution. It is concluded that there is a need for further comprehensive and systematic study of the problem of cybercrime with the use of legal psychology.

Keywords: cybercrime; legal psychology; cyber psychology; cyberspace; fight against cybercrime; psychology of cyber criminals.

● **Crime in the Field of High Information and Communication Technologies: An Analysis of the Regional Judicial and Investigative Practices.**

Svetlana P. Kushnirenko – PhD in Law, Associate Professor in the Department of Criminal Procedure and Criminalistics at the Saint-Petersburg State University Faculty of Law.

The article presents the results of the analysis of judicial and investigative practices in Saint-Petersburg and Leningrad Region in cases of crimes committed in the area of high information and communication technologies. A low crime rate is stated, which has no tendency to growth, while maintaining a significant latency. Statistics for the period 2006-2012, and structural analysis of the given category of crimes are provided. The analysis revealed the features of institution of proceedings and investigation of crimes under discussion, including analysing the committed errors, classified into unrecoverable with termination of proceedings, and disposable to be corrected that are technical in nature and do not affect the outcome of the

case. The author analyses the main evidence used to establish the facts to be ascertained, the most significant of which are the way of committing the crime, the perpetrator, place and time of the offence, and the occurring of harmful effects. This study made it possible to conclude that there are objective prerequisites for further development of criminalistics theory, strengthening its impact on the efficiency of countering transnational crime in the field of high information technologies through the development of group methodology to investigate these crimes.

Keywords: crime in the field of high information and communication technologies; analysis of judicial and investigative practices; avoidable and inevitable investigation errors; development of group methodology of crime investigation.

- **Investigation of Fraud Committed Using Modern Information Technologies.**

Anna A. Lebedeva – PhD in Law, Researcher at the All-Russia Scientific Research Institute of the Ministry of Internal Affairs of the Russian Federation.

The article describes the key points in the investigation of fraud committed using modern information technologies. It also considers the ways of committing crimes and investigative actions.

Keywords: investigation; fraud; Internet; investigative actions.

- **Certain Problems Associated with Obstructing the Investigation When Investigating into Crimes Committed with the use of Computer Technologies.**

Pavel V. Malyshkin – PhD in Law, Associate Professor in the Department of Criminal Law, Criminalistics and Criminology of the Law Faculty at the Mordovian State University named after N.P. Ogarev.

In the article, the author points out that the success of the investigation of crimes committed with the use of computer technologies depends on the success of overcoming resistance to this investigation, analysing the most typical methods of such opposition. Attention is drawn to the fact that resistance in the virtual space has its own characteristics and patterns that need to be taken into account in efforts to overcome it. Methods of crime concealment and their relationship to crime commission methods are also considered.

Keywords: crime concealment method; faking; crime commission method; detection, investigation, and solution of a crime.

- **Some Aspects of Creating the Scientific Basis for the Investigation of Crimes Involving the Use of Computer-Based Devices.**

Vladimir M. Meshkov – Doctor of Laws, Honoured Lawyer of Russia, Professor in the Department of Criminal Procedure, Criminalistics and Legal Informatics at Immanuel Kant Baltic Federal University.

Anatoly N. Grigoriev – Doctor of Pedagogy, PhD in Law, Associate Professor, Head of the Department of Administrative Law Disciplines and Information Support of Internal Affairs Agencies at the Kaliningrad branch of Saint-Petersburg University of the Ministry of Internal Affairs of Russia.

The article discusses some of the problematic issues around the formation of the scientific basis for the investigation of crimes committed using computer technologies. Special attention is paid to the various forms of activity of terrorist organizations on the Internet. The author justifies the need to create a federal bank of data on the experts in the field of computer technologies who may be involved in the investigation of such crimes, the development of special software for carrying out expert examinations in such matters, as well as to provide access to computer information of evidentiary nature.

Keywords: crimes involving the use of computer technology; Internet; terrorism; expert; technical computer examination; software.

- **Traces of Crime in the Field of High Technologies.**

Vladimir A. Meshcheryakov – Doctor of Laws, PhD in Technology, Professor in the Department of Criminalistics of the Law Faculty at Voronezh State University.

The article discusses the specific features of forming traces of crime in the field of high technologies. It examines the reasons for the different versions of their names and justifies the validity of the use of a 'virtual traces' category. On the example of the formation of digital traces of acoustic wave, the key features of virtual traces are illustrated.

Keywords: essence of virtual traces; virtual traces of sounds; properties of virtual traces.

- **Technique for Proving Transnational Cyber Fraud.**

Nadezhda G. Muratova – Doctor of Laws, Honoured Lawyer of the Republic of Tatarstan, Professor in the Department of Criminal Procedure and Criminalistics at Kazan (Volga Region) Federal University.

Igor O. Antonov – PhD in Law, Associate Professor in the Department of Criminal Procedure and Criminalistics at Kazan (Volga Region) Federal University.

The article examines the most significant aspects of the technique of proof in criminal cases of transnational cyber fraud. It identifies and describes the factors that have a significant impact on the effectiveness of the technique of proof in criminal cases of this category. The article reveals the significance of certain factors for effective proving of transnational cyber fraud, including (1) the adequacy of procedural regulation of the activity of law enforcement agencies to current threats; (2) the organisation of rational interaction at all levels of government agencies and non-governmental organisations specializing in the fight against transnational cybercrime; and (3) competent procedural and non-procedural efforts to detect traces of cyber fraud on the Internet.

Keywords: cyber crimes; cyber fraud; proof; investigation; international cooperation; operational and search activity; tracing activities; transnational crime; Internet.

- **Features of Structure and Content of the Methodology for the Investigation of Crimes Related to Information Resources Infringement.**

Gennady N. Mukhin – Doctor of Laws, Professor in the Department of Constitutional Law Disciplines at Belarus State Economic University.

Dmitry V. Isyutin-Fedotkov – PhD in Law, Associate Professor, Senior Lawyer at the "Voskhod" Research Institute.

The article focuses on the distinctive features of the content of techniques to investigate crimes that infringe on information resources. It justifies the opinion that the information about the specifics of the use of specialised knowledge in the detection and investigation of these crimes is particularly significant. An area of great complexity will be the stage of pre-investigation check of materials and identification of primary information on offences of this kind is. The definition is provided for the information and methodological basis of the detection and investigation of these crimes. The authors conclude that the main efforts of the judicial examination of evidence should be aimed at ensuring the reliability of the above mentioned information and the possibility to operate with it in the proof process in the case.

Keywords: methods of crime investigation; forensic characterisation of crime; computer crime; information and methodological basis of the investigation; prompt service of premises; protection of information resources.

- **Criminalistics Structure of Computer Crime Prevention Measures.**

Vitaly V. Polyakov – PhD in Law, Associate Professor in the Department of Criminal Procedure and Criminalistics at Altai State University.

The increasing number of crimes in the field of computer information arouses the need for the development and adoption of adequate measures to combat this phenomenon, and in the first place – within the context of criminalistics prevention of cybercrime. All preventive measures should be combined into the following main groups: of legal, institutional, technical, and methodical nature. The article analyses the content and features of preventive measures, and discusses their significance for the practice of law enforcement agencies and other organisations.

Keywords: criminalistics; prevention of crimes; computer crimes.

● **Illegal Actions with Potent and Toxic Substances Committed with the Use of the Internet.**

Lubov E. Chistova – PhD in Law, Associate Professor in the Department of Criminalistics at the Moscow University of the Ministry of Internal Affairs of Russia

The article discusses in detail the methods of illegal distribution and transfer with intent to distribute of potent and toxic substances through the Internet. Attention is drawn to the fact that the methods of commission of these criminal offences are characterised as fully structured, i.e. involving the preparation to commit a crime, the action itself aimed at bringing the criminal intent to completion, and the concealment of traces of the crime, as well as one's participation in it. The methods of distribution are considered in relation to different situations that may occur as a result of illegal purchasing of potent and toxic substances through online shops.

Keywords: potent and toxic substances; illegal distribution and transfer; online shops; preparation to commit a crime; methods of commission of a crime; methods of concealing criminal acts.

FORENSIC EXPERT EXAMINATIONS

● **On a Standard Technique for the Examination of Data Held in Mobile Phones.**

Olga V. Tushkanova – Head of the Department of Computer Examinations and Technologies at the Forensic Science Centre of the Ministry of Internal Affairs of the Russian Federation.

The article deals with the development of a standard technique for the “Examination of data held in mobile phones”. It describes the approaches to mobile communication devices systematisation, the study of typical tasks that arise when examining the data held in mobile phones, as well as the capabilities of the existing tools designed to examine data held in mobile phones, summarizing the experience of researching data held in mobile phones. Methods developed for experts in forensic computer examination are provided.

Keywords: mobile phones; standard technique; computer forensic examination.

● **International Cooperation in the Field of Forensic Computer Investigations.**

Shamil N. Khaziev – PhD in Law, Associate Professor, Senior Researcher in the Sector of Criminal Justice Problems at the Institute of State and Law of the Russian Academy of Sciences.

The article is devoted to the topical issues of international cooperation in the field of forensic investigations of computers and digital evidence. It presents a summary of the history of forensic computer investigation. It is noted that the development of forensic computer investigation in modern conditions is impossible without the international cooperation of experts and forensic institutions. Such cooperation is being strengthened and implemented in such forms as the establishment of international professional associations of forensic experts specialising in the field of computers and computer information, the organization of international scientific and practical conferences, the publication of international journals related to forensic computer examinations, as well as conducting international training workshops and courses for beginners and advanced experts. In addition, there are forensic

computer unit created within the framework of international law enforcement agencies and organisations, as well as in the previously established multidisciplinary forensic associations. Active exchange of useful methodological and technical information also takes place at international exhibitions devoted to new developments in computer technology. The largest contribution to the development of modern methods and technical means of forensic computer investigation has been made, in the author's opinion, by the recently created international association of experts in the field of forensic examination of computers, computer and information technologies, including the International Association of Computer Investigative Specialists; the Information Security and Forensics Society; the International Society of Computer Forensic Examiners; the International Information Systems Forensics Association; and the Working Group on Forensic Information Technology of the European Network of Forensic institutions; as well as computer forensics units of Interpol and Europol.

Keywords: computer expert examination; international cooperation; international organisations; computer technologies; criminalistics.

LAW ENFORCEMENT AGENCIES

● **Cybercrime: A View from Europe.**

Anatoly K. Kiselev – Doctor of History, Associate Professor, Head of the Department of History and Constitutional Law at the North-Caucasian Social Institute.

The article discusses the different definitions of the term 'cybercrime'. It analyses the growing threats from computer crime. In addition, it tells a story about the creation in 2013 in the framework of the European Union of the new international agency to combat cybercrime.

Keywords: cybercrime; phishing; industrial espionage; child pornography on the Internet; police; Europol; international cooperation; European Cybercrime Centre (EC3).

● **Legal and Organizational Support for the Detection and Investigation of Crimes in the Field of Computer Information: Current State and Ways for Improvement.**

Ivan A. Popov – Doctor of Laws, Professor, Senior Research Fellow of the Fifth Research Center for Criminal and Procedural Legislation Development and Research on Issues of Preliminary Investigation at the All-Russian Research Institute of the MIA of Russia.

The article analyses the effectiveness of the implementation of legal rules on liability for crimes in the field of computer information taking into account the recent changes and amendments introduced by the legislator. The problems of organizational support for the detection and investigation of this category of crime are discussed, as well as improvement of procedural interstate cooperation in the fight against it.

Keywords: computer information; interagency information interaction; software and hardware; unified database; internet technology; international cooperation; procedural interaction.

● **Special Units and Organizations to Combat Internet Fraud in Different States of the World.**

Victor P. Sabadash – PhD in Law, Associate Professor, Head of the Department of Criminal Law and Justice at Zaporozhye National University.

The article examines the topical issues of combating cyber crime through analysis of activities of special units operating within public and private sectors in the leading countries of the world, including the USA, the UK, Russia, France, Germany, and some other countries that have great experience in establishment and functioning of such units and organisations, which can be used to create similar structures in other countries. It is stated that today some special organisations have already been created to deal with different aspects of Internet fraud, and they can be divided into three large groups. The first group involves organisations and departments, created by governments as part of central authorities, including ministries, departments,

security services, etc. The second group comprises special organisations and expert teams focusing on the study of computer incidents and recording Internet crime complaints. As regards the third group it consists of special organisations created within the framework of international and intergovernmental institutions.

Keywords: Internet fraud; fight; resistance; special units; special organisations; investigation; crime; cyber crime; information technologies.

INTERNATIONAL CRIMINAL LAW AND JUSTICE

● **International Legal Regulation of Cooperation in the Fight against Internet Crime.**

Roman I. Dremluiga – PhD in Law, Associate Professor in the Department of International Public and Private Law at the Far Eastern Federal University.

The article focuses on the analysis of the present state of international legal regulation in the field of combating Internet crime. The author attempts to find the way of how to overcome transborderness of this kind of criminal activity, arriving at the conclusion about the need for new international sources of regulation be created. In addition, the article also analyses the shortcomings of the existing proposals of legal science relating to international legal regulation of the fight against Internet crime.

Keywords: Internet crime; transboundary offences; international criminal law.

● **A Comparative Analysis of International Treaties on Combating Cybercrimes (with Respect to their Criminalising Provisions).**

Konstantin P. Zadoya – PhD in Law, Associate Professor in the Department of Criminal Law and Criminology at Taras Shevchenko National University of Kyiv.

The article reviews the provisions of international treaties on combating cybercrimes. The author points to the importance of such agreements in harmonizing the provisions of national criminal laws. A list of the existing treaties on combating cybercrime is given. Those agreements contain different listings of cybercrime types. Furthermore, the same types of cybercrime are characterized differently.

Keywords: cybercrime; international agreement; computer information; information technology; computer system.

COMPARATIVE JURISPRUDENCE

● **Criminal Law Tools to Combat Cyber Crime in the European Continental System of Law.**

Sofja I. Veibert – PhD in Law, Assistant Professor in the Department of Criminal Law Disciplines at the Ural Institute – Branch of the Russian Presidential Academy of National Economy and Public Administration.

While currently there is a rapid growth of cybercrime, so there is a need to assess the effectiveness of the existing set of tools to counter this threat. The article classifies and analyzes offenses relating to cybercrime. The normative criminal law regulations of the EU member states are investigated from the perspective of comparative law, as it is criminal legislation that determines the wrongfulness and punishability of acts. Prospects for future development of normative regulations criminalizing cybercrime are also identified.

Keywords: cybercrime; criminal law; European Union; European continental system of law; 'computer' crimes.

● **Theoretical and Legal Issues of the Classification of Crimes Involving the Use of Computers (Based on the Criminal Law of Ukraine).**

Ninel V. Marchenko – PhD in Law, Judge of the Zavodsky District Court of the City of Zaporozhye.

The article identifies and analyses the most problematic theoretical and legal issues that arise within law-enforcement agencies in the classification of crimes committed through the use of computers. Suggestions are offered for improving the criminal legislation of Ukraine in order to ensure the effectiveness in the fight against this scourge.

Keywords: classification of crimes; computer equipment; automated systems; electronic computers; criminal liability; information.

● **Cyber Security of the Individual as a Priority of the State Policy of Ukraine in the Field of Information and the Role of Criminal Law in Its Implementation.**

Vladimir V. Shablisty – PhD in Law, Associate Professor in the Department of Criminal Law and Criminology of the Investigators Training Faculty at Dnepropetrovsk State University of Internal Affairs.

The article focuses on the justification of the author's definition of cyber security of the individual as part of his information security from the perspective of the person, rather than the state. The absolute majority of all modern studies of cyber security handle it as an integral part of the national or state security, which is unacceptable for the author because the Constitution of Ukraine declares the individual to be the highest social value in the state. The author argues that the current version of the criminal law is not able to fully ensure the right of every person to freely meet their information needs and therefore it needs qualitative and quantitative changes.

Keywords: individual; safety; information; cyber security; criminal law; science.

PESONALIA

● **Marking the 75th Birthday of Sergey Petrovich Scherba**

Authors Information

Manuscripts Submission Guidelines