How to Cite:

**Electronic Evidence: Problems of Application in Practice in Proving Crimes in the Field of Turnover of Drugs, Psychotropic Substances**

**Dmytro Golovin**
Odesa State University of Internal Affairs, Odesa, Ukraine

**Yehor Nazymko**
Donetsk State University of Internal Affairs, Mariupol, Ukraine

**Oleh Koropatov**
Odesa State University of Internal Affairs, Odesa, Ukraine

**Maksym Korniienko**
Odesa State University of Internal Affairs, Odesa, Ukraine

**Abstract**—Relevance of the problem outlined in the article is due to increasing levels of crime in the sphere of illicit trafficking in narcotic drugs, psychotropic substances, their analogues or precursors using information and telecommunication systems. The aim of the article is a comprehensive analysis of the problem of the use of electronic evidence in proving crimes of trafficking in narcotic drugs, psychotropic substances, their analogues or precursors. To achieve the goal were used to theoretical, historical comparative methods and logical analysis; application of dialectical method allowed to reveal the meaning of concepts *electronic evidence* The article presents the most common methods of communication in the sale of drugs, psychotropic substances, their analogues or precursors through such means of communication as messengers, social networks, online games, proprietary programs. It is established that the main causes of drug trafficking crimes include: insufficient legal regulation of cyberspace, the lack of geographical boundaries, the spread of information about drugs on the Internet, especially in Darknet), the uncontrolled development of the cryptocurrency market. The definition of electronic proof in the Ukrainian legal system, as well as the forms and features of electronic proof are considered. The judicial practice of the Supreme Court of Ukraine regarding the recognition of electronic proof as appropriate evidence in cases is disclosed. The materials presented in the article will be useful for review and study by students, cadets,
graduate students, assistant professors, teachers, employees of judicial and law enforcement agencies.

**Keywords**—criminal process, drugs, electronic evidence, information technologies, narcotic, psychotropic.

**Introduction**

Over the past decade, Ukraine has made significant strides in informatizing society, as evidenced by statistics from Global Logic, which found that 60% of Ukraine’s population is already registered on social networks, the most popular of which is YouTube with 96% of users. As for the dynamics of growth, from the beginning of 2020 to the beginning of 2021 the Ukrainian audience of social networks increased from 19 million to 26 million users, for example by 7 million people (During the quarantine year the number of Ukrainians on social networks increased by seven million, 2021).

At the state level, the development of informatization in our country is considered one of the national priorities, as exemplified by the mobile application, web portal and brand of the digital state, developed by the Ministry of Digital Transformation of Ukraine - DIIA, which has an ambitious goal to translate 100% of public services online (DIIA (service), 2021). And according to the Minister of Digital Transformation of Ukraine M. Fedorov, over the next two years in Ukraine electronic voting tools may be introduced that will operate during referendums and elections. But along with the absolutely necessary information changes in the public life of every person, it is natural that there are new schemes of illegal behavior of criminal elements, to which the law enforcement system must respond and such a reaction must be on a par with modern information technology, which unfortunately almost never is happening, and this is a problem not only of Ukraine, but a global problem (Bitzer et al., 2016).

The public danger of crimes in the sphere of illegal circulation of drugs and their analogues, committed using computer technologies, is determined along with other signs of an increase in the criminality of the information space of the global network, influencing various spheres of society and causing inappropriate social and criminal behavior of groups of people or individuals (Movchan et al., 2021). This is due to the general availability, openness of the global network, and insufficient legal regulation of its activities. It can be stated that the criminal elements are the first to have the most advanced software, they have the opportunity to hire the most professional workers, as well as to operate in different legal systems of different countries (McCarthy & Hagan, 1995).

For example, the UN Program on International Drug Control and Crime Prevention contains the Model Law on the Punishment of Drug-Related Crimes, which prohibits the use of computer data exchange networks to facilitate or advance the production, manufacture, trafficking and illicit use of drugs (Zuccato et al., 2000). In some foreign countries, the use of the global network in the commission of crimes in the sphere of illicit drug trafficking is criminalized either as a mandatory sign of the main corpus delicti, or as a qualifying sign. This
testifies to the increased attention of the world community to the problem of drug
distribution via the Internet. It should be noted that the main source of law in the
countries of the Romano-Germanic legal family, including Ukraine, is a legal act,
and the legal norm is considered as an abstract, general and impersonal rule of
contact that can be repeatedly applied to an indefinite number of cases and
persons (Pickett & Ryon, 2017).

Electronic evidence and the issue of their use in the judicial process of Ukraine
remain controversial issues in the legal community (Nugraha et al., 2020). The
very concept of "electronic evidence" appeared in the 70s of the twentieth century,
since the advent of machine documents. According to Art. 2 of the Model Law on
Electronic Commerce of 1997, recommended by the UN General Assembly, it is
defined as information prepared, sent, received or stored by electronic, optical or
similar means, including electronic data exchange, e-mail, telegraph or fax. As for
the typical scheme of committing crimes in the field of trafficking in narcotic
drugs, psychotropic substances, their analogues or precursors, it has undergone
significant changes over the past 10 years (Colleoni et al., 2000). The results of
human activity are increasingly reflected in electronic (digital) form, including
those that acquire the meaning of legal facts. There are no more real meetings for
the sale of drugs, all communication has passed for anonymity online. Therefore,
the share of drug sales is made through such means of communication as
messengers (Telegram, Viber, WhatsApp and Signal), social networks (VKontakte,
Odnoklassniki, Instagram, Facebook and Twitter), online games (Counter Strike,
DOTA, Overwatch, World of Warcraft, Rainbow 6 Siege, Apex, Battlefield and Call
of Duty), proprietary programs (Discord, TeamSpeak and Raidcall). Therefore, the
issue of the use of electronic evidence is especially relevant in the investigation of
crimes in the field of trafficking in narcotic drugs, psychotropic substances, their
analogues or precursors (Ankier, 1974; Hartford et al., 2019).

Analysis of the current reality in the field of procedural law of Ukraine
(Studennukov, 2019; Zavudniak, 2019) shows its transformation into case law,
when the court's own conviction takes precedence over legal norms formed so that
it is impossible to consider them as a unified tool for establishing the truth.
Indicative in this aspect, in our opinion, the use of electronic evidence in criminal
proceedings. In 2016, a dissertation was defended for the degree of Candidate of
Law on the topic "Electronic means of proof in civil proceedings", the author –
A. Iu. Kalamaiko. A new dissertation research in this direction is currently being
carried out by O. Iu. Gusev. Various aspects of electronic evidence in criminal
procedure legislation have been studied by a number of scholars. But there are
still a number of practical and scientific inconsistencies regarding electronic
evidence and their recognition as appropriate and admissible in court, which led
to our study (Ramadani et al., 2021).

Methodological Framework

The purpose of the article is a comprehensive analysis of the problem of using
electronic evidence in proving crimes in the field of trafficking in narcotic drugs,
psychotropic substances, their analogues or precursors (Reilly et al., 2000). The
study was conducted on the basis of practical experience gained in senior
positions of the Main Directorate of the National Police of Ukraine in Odessa
region during the implementation of professional activities, as well as during scientific and pedagogical activities in higher education institutions of the Ministry of Internal Affairs of Ukraine.

To achieve this goal, a number of scientific methods were used, namely: theoretical – to study and analyze official documentation, scientific and methodological and educational literature, generalization of information to determine the theoretical and methodological foundations of the study; logical analysis – to formulate the basic concepts and classification; concrete-historical – to demonstrate the dynamics of development use of electronic evidence in criminal proceedings; the application of the dialectical method allowed to reveal the meaning of the concepts "electronic proof", "electronic traces"; to find out the signs of electronic evidence, as well as to establish the content and features of the constituent elements of the implementation and application of electronic evidence in law enforcement; empirical methods for generalization of practical experience, observation and discussion (Nyandra et al., 2018).

The formal-legal method was used in the analysis of current national legislation, identifying inherent advantages and disadvantages in the use of electronic evidence, as well as formulating proposals to improve the procedural use of evidence in electronic form in Ukraine. The theoretical basis of this study were the works of domestic and foreign scholars, their fundamental achievements in the sciences of administrative, criminal, civil law, as well as encyclopedic legal literature (Shomirzayev, 2021).

**Results**

The current state of crime in the sphere of illegal drug trafficking, including those committed using the Internet, is characterized by a high level of latency. This is due to the lack of mechanisms for automatic detection of resources on the network containing illegal information about drugs, or used for illegal activities with them, as well as identification of offenders. The emergence of such resources is monitored and analyzed using search engines and the result depends on the development of information retrieval, on the one hand, and what encryption programs are used by offenders. In addition, in the case of identification of sites on the Internet used for the distribution of drugs and involvement in their consumption, which are registered outside the territory of Ukraine, it becomes difficult to prosecute the owners of such resources. As a rule, the only measure applied to the owners of prohibited resources on the Internet is to restrict access by providers.

Also, such activities can be conducted from the territory of Ukraine, with the establishment of access restrictions for the Ukrainian consumer, but only to other countries, which significantly limits Ukrainian law enforcement officers in the methods of detecting such activities. The use of the possibilities of the Internet in the commission of crimes in the sphere of trafficking in narcotic drugs, psychotropic substances, their analogues or precursors has undergone significant changes. The characteristic features of these acts include:

- the remote nature of illegal actions in the absence of physical contact between the drug dealer and the purchaser; the person who posted
information about the manufacture or processing of drugs and the person who manufactures or processes them; the person who posted information aimed at inducement to the use of drugs, and the person who is being persuaded;

- increased secrecy of the commission of a crime, provided by the specifics of the network space (developed mechanisms of anonymity, the complexity of the infrastructure);
- the cross-border nature of drug crimes, in which the perpetrator, the object of the criminal offense and (or) the victim may be under the jurisdiction of different states;
- high preparedness of offenders, the intellectual nature of their illegal activities (preparation and commission of drug crimes require special knowledge and skills);
- the special nature of the crime scene. Traces of criminal actions are distributed over a variety of objects (computer systems of the criminal, provider; intermediate network nodes, etc.);
- non-standard, complexity, diversity, frequent updating of the ways of committing drug crimes and the special means used, including the development of the cryptocurrency market);
- multi-episode nature of illegal actions;
- the possibility of committing a crime in an automated mode, the implementation of complex scenarios by one person when combining the resources of individual computers;
- the absence of witnesses of illegal actions as persons who observed the event of the crime and who are able to identify the offender.

Before considering the peculiarities of proving crimes in the field of trafficking in narcotic drugs, psychotropic substances, their analogues or precursors, it is necessary to explore the very concept of "electronic evidence", because there is a problem of insufficient fixation in Ukrainian legislation. Therefore, in accordance with Part 1 of Art. 100 Civil Procedure Code of Ukraine electronic evidence is information in electronic (digital) form, containing data on the circumstances relevant to the case, in particular, electronic documents (including text documents, graphics, plans, photographs, video and audio recordings, etc.), websites (pages), text, multimedia and voice messages, metadata, databases and other data in electronic form. Such data can be stored, in particular, on portable devices (memory cards, mobile phones, etc.), servers, backup systems, other places of data storage in electronic form (including the Internet) (Civil Procedure Code of Ukraine, 2004).

Also in accordance with paragraph 3 of Part 2 of Art. 99 of the Criminal Procedure Code of Ukraine, the documents may include media on which procedural actions are recorded by technical means, if they are compiled in the manner prescribed by the CPC of Ukraine. In Part 4 of Art. 99 of the CPC of Ukraine states that a duplicate of the document (a document made in the same way as its original), as well as copies of information contained in information (automated systems, telecommunications systems, information and telecommunications systems, their integral parts, made investigator, prosecutor with the involvement of a specialist, are determined by the court as the original document.
According to art. 84 of the CPC of Ukraine evidence in criminal proceedings are factual data obtained in the manner prescribed by this Code, on the basis of which the investigator, prosecutor, investigating judge and court establish the presence or absence of facts and circumstances relevant to criminal proceedings and subject to proof. Procedural sources of evidence are testimony, physical evidence, documents, expert opinions (Criminal Procedure Code of Ukraine, 2012). Among the definitions provided by scientists, the most common among them are: O. I. Kotliarevskyi, V.V. Muradov, D. M. Kytsenko electronic evidence means a set of information stored electronically on any type of electronic media and electronic means (Alieksieieva-Protsiuk & Bryskovska, 2018), electronic evidence means evidence in criminal proceedings in electronic form (Volkov, 2018).

The concept of "electronic traces" is also reflected in the domestic forensic literature. Yes, according to G. Avdeeva and S. Storozhenko, electronic digital traces are material invisible traces, which can be detected, recorded and studied by digital electronic devices and which contain any forensic material information (information, data) recorded in electronic digital form on physical media. This definition focuses on the principles of working with electronic traces, but, unfortunately, lacks due attention to reveal their nature. A more thorough definition of this concept was proposed by foreign scientists V. Vekhov, B. Smahorynskyi, and S. Kovalev: electronic trace is any criminologically significant information, for example information (messages, data) presented in the form of electrical signals, regardless of the means of their storage, processing and transmission. Mechanism their formation is based on the electromagnetic interaction of two or more objects. Recognizing the value of the work of these authors on the mechanism of formation of such traces, we cannot agree with the above wording in terms of identifying the trace with the information it carries.

In general, the scientist V. Vekhov developed the basics forensic doctrine of computer information and means of its processing, proposing its author’s definition. Interestingly, in this work, the scientist is none does not use the term "electronic proof", having come to it only in 2013-2016. In addition, it should be noted that both the criminal procedure legislation and the scientific doctrine of some foreign countries, compared to domestic ones, are currently at a slightly higher level of development in relation to electronic sources evidentiary information. At the beginning of the development of computer technology, the problem of using digital information in evidence arose in the United States, where at that time the rules for the use of "novel evidence" were innovated. According to the peculiarities of the Anglo-Saxon legal system, the source of such rules is the case law in the case of Frye vs United States, which concerned the use of new data and methods of science in evidence and consisted of two elements: first, the court must determine which field of scientific knowledge data and techniques that underlie the evidence, and secondly, whether the leading scientists in this field recognize the principle on which the evidence is formed (Tsekhan, 2013). It is also necessary to pay attention to the consolidation of the concept of electronic document in Art. 371a of the German Code of Civil Procedure, which includes any information and electronic form, the contents of which can be read repeatedly using written signs, in electronic documents (Yesimov, 2016).
Discussion

There are also differing views on the place of electronic evidence in the system of procedural sources of evidence. A. S. Bilousov as one of the varieties of a separate group of physical evidence proposes to consider computer objects (Bilousov, 2008). Professor Yuri Orlov and S. S. Cherniavskyi believe that the criterion for relation to criminal proceedings electronic reflections are similar to physical evidence (Orlov & Cherniavskyi, 2017). A. V. Stolitnii and A. V. Kalancha make conclusion and emphasize that the document as a source of evidence in criminal proceedings can be in both paper and electronic form. D. M. Tsekhan argues that digital information and its media, taking into account the unique characteristics (especially intangible) cannot be attributed to any qualification group (Tsekhan, 2013).

Also D. M. Tsekhan notes that when detecting digital information, investigators have many difficulties in capturing it, taking into account the requirements of criminal procedure law for evidence and further use in criminal proceedings. This is due to the ability to quickly change the content of the site, the physical location of servers in other countries, the use of anonymous software (Tsekhan, 2013). V. V. Markov and R. R. Savchenko determine the absence of grounds for inadmissibility of electronic evidence obtained from any digital media, and the legal order obtained in accordance with the Criminal Procedure Code of Ukraine (Mapkov & Savchenko, 2014).

G. Chyhryna singles out the lack of knowledge of the subjects of evidence in the field of computer hardware and software, the need to develop and improve existing special training programs that would provide law enforcement officers in the use of computer equipment and technology to work with media computer (electronic) information, detection, analysis, imaging and use of computer information (Chyhryna, 2017). V. V. Muradov also notes that due to the lack of basic knowledge in the field of IT and a well-established method of collecting and using such evidence, it is necessary to involve specialists (and appoint examinations), remove a large amount of equipment or spend a lot of time searching and fixing them (Muradov, 2013). Thus, for electronic evidence, the following features can be identified: existence in intangible form; the need to use certain technical means for reproduction; the ability to transfer or copy to different devices without losing performance; the original electronic proof can exist in many places at the same time.

In particular, A. Yu. Kalamaiiko identifies the following features: "1) the impossibility of direct perception of information, which necessitates the use of hardware and software to obtain information; 2) the presence of a technical storage medium that can be used repeatedly; 3) a specific process of creating and storing information, which allows you to easily change the media without losing content and vice versa, provides the ability to make changes to the content without leaving traces on the media; 4) the absence of the concept of "original" electronic means of proof due to the complete identity of electronic copies; 5) the presence of specific "details", the so-called metadata – information of a technical nature, which is encoded within the files" (Kalamayko, 2016).
In our opinion, there is no need to single out electronic evidence as an independent procedural source of evidence, but it is necessary to clearly define the electronic form of fixation, which will be integral and unchangeable, and therefore need to define in regulations the algorithm of obtaining, recording, using, storing and analyzing. In addition, certain algorithms should be immediately introduced into the curricula of higher education for the formation of high-quality modern knowledge and skills in the field of information and telecommunications. When working with electronic evidence, certain principles must be followed:

- Legality. Employees of law enforcement agencies conducting investigate and investigate evidence in electronic form, the obligation to comply current legislation, general procedural and forensic principles.
- Data integrity. The actions of the specialist should not lead to material changes in the data, electronic devices or media that can be used as evidence.
- Documenting the process. Document any actions performed in relation to electronic evidence, and store these documents in case of verification to be independent a third party could repeat these steps and get a similar result.
- Expert support. If it is assumed that during the inspection (search) may be detected electronic evidence, receive support from specialists (specialists), providing if possible, their presence at the scene.
- Appropriate professional training. If in the process of inspection (search) there are no specialists
- From electronic evidence, priority actions at the scene are carried out by persons who have the necessary knowledge and skills to identify and gather evidence.
- Reasonable caution. Avoid any intentional or unintentional actions that can damage potential evidence presented in digital form (Ponomarev, 2011).

So let’s move on to practical analysis. Due to the fact that today the sale of narcotic drugs, psychotropic substances, their analogues or precursors mostly takes place through messengers, in this context the case of the Supreme Court of the Judicial Chamber of the Civil Court of Cassation No. 753/10840/19 where there was investigating whether a screenshot of messages from the phone can be proper proof. The plaintiff stated that in the correspondence between her ex on the phone concerning organizational meetings with her son, he had made open threats, insults, humiliation of honor and dignity, used obscene language, called obscene words of the applicant, her relatives, used obscene language normal human communication (Maes et al., 1997).

The court of first instance upheld the claim in part. A restrictive order has been issued. The following measures of temporary restriction of rights for a period of 6 months are established: it is forbidden to conduct correspondence, telephone conversations and in any way communicate or communicate through other means of communication with the applicant and the child personally and through third parties. The Court of Appeal upheld the decision of the court of first instance. Disagreeing with the court’s decision, the ex-husband filed a cassation appeal. Considering the case, the Supreme Court referred to Part 1.3 of Art. 100 CPC of Ukraine, which we previously cited and further noted that such data may
be stored, in particular, on portable devices (memory cards, mobile phones, etc.), servers, backup systems, other places of data storage in electronic form (including the Internet). The parties to the case have the right to submit electronic evidence in paper copies, certified in the manner prescribed by law (Civil Procedure Code of Ukraine, 2004). A paper copy of an electronic proof is not considered written proof. Thus, the SCU emphasized that in support of the claims the applicant had provided screenshots of telephone and tablet messages, Viber printouts which the trial court, with which the appellate court had agreed, considered appropriate and admissible evidence examined by the courts as a whole legal assessment.

Having established that the content of specific phrases, vocabulary and the nature of the use of language used by the former in correspondence with his ex-wife and young son, gives grounds to conclude that his actions should be classified as domestic violence, the court reasonably prohibited him from correspondence, telephone conversations and in any way to communicate or communicate through other means of communication with the former and injured child personally and through third parties. Thus, the Supreme Court dismissed the cassation appeal and upheld the decision of the court of first and appellate instance, recognizing the screenshots of the notices as evidence in the case (SCU case No. 753/10840/19 of 13.07.2020).

Contrary to the above-mentioned decision of the Supreme Court of Ukraine in case No. 922/51/20, the Supreme Court noted that when an electronic copy of a written evidence is not considered electronic evidence. Thus, in the cassation appeal, the cassator pointed out that the cassation appeal concerns the issue of law, which is fundamental for the formation of a unified law enforcement practice, namely - the use of electronic evidence in the form of electronic correspondence, including messengers (Skype, Viber and WhatsApp). He also pointed out that correspondence via messengers (in the form of text and multimedia messages) fully meets the requirements of electronic proof.

However, in response to the cassation appeal, the defendant considers unfounded the plaintiff's arguments about the existence of a contractual relationship between them. Thus, the defendant pointed out that the plaintiff provided the court with electronic correspondence, screenshots, copies of documents to confirm his arguments, which cannot be considered appropriate evidence. The SCU noted that if a copy (paper copy) of the electronic evidence is submitted, the court may, at the request of the party to the case or on its own initiative, request the original electronic evidence from the person concerned. If the original electronic evidence is not submitted, and the party to the case or the court questions the compliance of the submitted copy (paper copy) of the original, such evidence is not taken into account by the court (Part 5 of Article 96 of the Code of Civil Procedure of Ukraine). The SCU also concluded that the party to the case has the right to submit electronic evidence in the following forms to substantiate his claims and objections: 1) the original; 2) an electronic copy certified by an electronic digital signature; 3) a paper copy certified in the manner prescribed by law.
A paper copy of an electronic proof is not considered written evidence, but is one of the forms in which a party to the case has the right to submit electronic evidence. Thus, the submission of electronic evidence in a paper copy does not make such evidence inadmissible. The court may not take into account a copy (paper copy) of the electronic evidence, if the original electronic evidence is not submitted, and the party or the court questions the responsibility of the submitted copy (paper copy) of the original (case of the Supreme Court of Ukraine from 29.01.2021 No. 922/51/20).

It should also be noted that on February 14, 2019, the Grand Chamber of the Supreme Court, reviewing the case No. 9901/43/19, decided that the electronic digital signature is the main requisite of this form of electronic evidence. The absence of such details in the electronic document excludes grounds to consider it original, and therefore appropriate evidence in the case (case of the Supreme Court of Ukraine dated 14.02.2019 No. 909901/43/19). A similar legal position was expressed by the Supreme Court in the decision of 19.12.2018 in the case No. 226/1204/18, from 04.12.2018 in the case No. 2340/3060/18, from 23.11.2018 in the case No. 813/1368/18, dated 14.12.2018 in case No. 804/3580/18. Therefore, both the original and a copy of the electronic document must be certified by Single Digital Signature.

**Conclusion**

The main reasons for drug crimes on the Internet include: insufficient legal regulation of cyberspace, lack of geographical boundaries, dissemination of information about drugs on the Internet, especially on the Darknet), uncontrolled development of the cryptocurrency market. The main conditions for drug crimes on the network include: anonymity, public availability of information disseminated via the Internet, virtualization (lack of material component when working on the Internet), lack of methodological developments in the investigation of law enforcement agencies, improper organization of the work of telecommunication service providers (providers). In today’s conditions, the use of electronic means of proof, their admissibility and probative value are becoming increasingly important. In practice, and especially when proving crimes in the field of trafficking in narcotic drugs, psychotropic substances, their analogues or precursors, as this type of illegal activity has almost completely gone online, there are many questions about the possibility of using information from messengers, social networks, network games or proprietary programs. In the course of the research, we came to the conclusion that the issues of electronic evidence are poorly regulated by law, and especially by the Criminal Procedure Code.

According to the practice of the Supreme Court of Ukraine, electronic evidence can be stored, in particular, on portable devices (memory cards, mobile phones, etc.), servers, backup systems, other places of data storage in electronic form (including the Internet). According to the above provisions, the original electronic document is an electronic copy of the document with the required details, including the electronic signature of the author. Messenger correspondence (in the form of text and multimedia messages) fully meets the requirements of electronic proof. However, the court may not take into account a copy (paper copy) of the electronic evidence, if the original electronic evidence is not
submitted, and the party to the case or the court questions the responsibility of the submitted copy (paper copy) of the original.

Also, in our opinion, there is no need to distinguish electronic evidence as an independent procedural source of evidence, but it is necessary to clearly define the electronic form of fixation, which will be integral and unchangeable, and therefore need to define in regulations the algorithm for obtaining, recording, using, storing and analyzing. The independence of the concept of electronic evidence depends on the characteristics of the data carrier. In addition, certain algorithms should be immediately introduced into the curricula of higher education for the formation of the latest high-quality modern knowledge and skills in the field of information and telecommunications.

To achieve the aim an appropriate procedural form is necessary which would let the judge and other parties to the process insure as conveniently and effectively as possible to show and try true conditions of the case and to clear the necessary evidence to make information technologies serve the litigation purposes more effectively (Lluch, 2011; Chiasson et al., 2007). The solutions to those questions are closely linked to the understanding of the electronic evidence essence, as well as to determine its place in the trial process. Thus, the current negative trends of drug-related crime on the Internet, the peculiarities of its existence and reproduction in the global network dictate the need for further deeper research into the criminological characteristics of the crimes under consideration and the grounds for criminalizing the method of drug distribution.

References


