UDC 343.98
IRSTI 10.85.01

D.P. Utepov
The Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Nur–Sultan c., the Republic of Kazakhstan

DIGITAL INFORMATION AS PROOF IN CRIMINAL PROCEEDINGS

Abstract. In the 21st century, the century of information technology, we are surrounded by many devices that have various functions for interacting with digital information, which is fundamentally different from analog information. Digital information can be created, stored, received and transmitted by electronic computers in binary computing system through encoding, which opens up new avenues for crimes. For example, in the Republic of Kazakhstan there is an increase in the number of crimes committed with the use of computer technology and technical means. These features of digital information require law enforcement agencies to adapt to the requirements of the time. This article provides a comparative analysis of the opinions of domestic and foreign authors on the use of digital information as evidence in criminal proceedings. In addition, the possibility of using digital information instead of computer information is considered. The author, discussing the basis of digital information and its features, came to the conclusion that it is necessary to include it in the legislation of the Republic of Kazakhstan.

Keywords: digital information; computer information; evidence; computer crimes; binary code; analog information; electronic media; IT–technologies.

Д.П. Өтепов
Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы, Нұр–Сұлтан қ., Қазақстан Республикасы

ҚЫЛМЫСТЫҚ ІС ЖҮРГІЗУДЕ ДӘЛЕЛДЕМЕ РЕТІНДЕГІ САНДЫҚ АҚПАРАТ

Аннотация. XXI ғасырда – ақпараттық технологиялар ғасырында бізді аналогтық ақпараттан түбегейлі ерекшеленетін сандық ақпаратпен өзара әрекеттесудің әртүрлі функциялары бар көптеген құрылымдар қоршап жатыр. Сандық ақпаратты электронды есептеу машиналары екілік есептеу жүйесінде кодтау арқылы құруға, сақтауға, қабылдауға және беруге болады, бұл шабуыл жасаудың жаңа жолдарын ашады. Мысалы, Қазақстан Республикасында компьютерлік техника мен техникалық құралдарды пайдалану арқылы жасалған қылмыстардың санының артуы проблемасы байқалады. Сандық ақпараттың бұл ерекшеліктері құқық қорғау органдарынан уақыт шындығына бейімделуді талап етеді. Бұл мақалада отандық және шетелдік авторлардың қылмыстық іс жүргізудегі дәлел ретінде сандық ақпаратты пайдалану туралы пікірлеріне салыстырмалы талдау жасалды. Сонымен қатар компьютерлік ақпараттың орнына сандық ақпаратты пайдалану мүмкіндігі қарастырылады. Автор цифрлық ақпараттың негізін және оның ерекшеліктерін талқылай отырып, оны Қазақстан Республикасының заңнамасына енгізу қажеттілігі туралы қорытындыға келді.

Түйінді сөздер: сандық ақпарат; компьютерлік ақпарат; дәлелдеме; компьютерлік қылмыстар; екілік код; аналогтік ақпарат; электрондық жеткізгіш; IT–технология.

Д.П. Утепов
Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Нур–Султан, Республика Казахстан

ЦИФРОВАЯ ИНФОРМАЦИЯ КАК ДОКАЗАТЕЛЬСТВО В УГОЛОВНОМ ПРОИЗВОДСТВЕ

Аннотация. В XXI веке – веке информационных технологий нас окружают множество устройств, имеющих различные функции взаимодействия с цифровой информацией, которая фундаментально отличается от аналоговой информации. Цифровая информация может создаваться, храниться, приниматься и передаваться электронными вычислительными машинами в двоичной вычислительной системе путем кодирования, что открывает новые пути для совершения преступлений. Например, в Республике Казахстан наблюдается проблема увеличения количества преступлений, совершенных с использованием компьютерной техники и технических

средств. Эти особенности цифровой информации требуют от правоохранительных органов адаптироваться к реáлиям времени.

В статье проведен сравнительный анализ мнений отечественных и зарубежных авторов об использовании цифровой информации как доказательство в уголовном производстве. Кроме того, рассмотрена возможность использования цифровой информации вместо компьютерной информации. Автор, обсуждая основу цифровой информации и ее особенности, пришел к выводу о необходимости ее включения в законодательство Республики Казахстан.

Ключевые слова: цифровая информация; компьютерная информация; доказательства; компьютерные преступления; двоичный код; аналоговая информация; электронный носитель; IT–технологии.

DOI 10.52425/25187252_2021_19_95

Information technologies have become an essential part of almost every segment of modern society. Computers in combination with IT technologies, communication devices and software technologies make automation and remote control of social life and its other aspects possible.

Currently unfolding State governmental program «Digital Kazakhstan» includes 17 different features: digitalization of internal services of governmental bodies, development of finance technologies and cashless payment systems, providing safety of data in information and communication technologies (ICT), expansion of communication network and ICT infrastructure, digitalization of vehicles and logistics, and others. This indicates that the country's law enforcement bodies' efficient and timely response to crimes is directly dependent on ICT.

Chapter 7 of the Criminal Code of Kazakhstan addresses criminal infraction in the scope of informatization and communication, while Section 16 of the Criminal Code of Ukraine considers criminal offenses related to the use of electronic computing machines (computers), systems and computer networks and telecommunication networks [1]. This feature is common in most of the CIS countries.

However, the list of criminal offenses addressed in Chapter 7 of the Criminal Code of Kazakhstan is by far not exhaustive, because not all possible types of crimes related to computer and electronic devices are covered. This fact is evident from the information provided by the Committee on the legal statistics and special accounts of the state office of public prosecutor of the Republic of Kazakhstan. For example, in 2020, 62 illegal acts that fall under Chapter 7 were registered, while the number of illegal acts committed with the use of computers and electronic devices totaled at 771 [2]. Furthermore, the number of registered illegal acts related to computers and electronic devices was 70 and 112 in 2018 and 2019 respectively, showing an increasing tendency.

Over time, it is becoming more difficult to distinguish «computer crimes» from other types of crimes due to the increasing versatility of used special equipment, software and electronic devices in these crimes.

Although the cases with ICT–related crimes, internet–frauds or crimes in the scope of informatization and communication that fall directly under Chapter 7 are easily resolved in the field of the Criminal Code of Kazakhstan, crimes needing «digital information» as evidence are less apparent to process.

For example, «on December 2, 2015, a man, born in 1965, made a call from his cell phone to the director of Karaganda Regional Highest Sisterly College, and, after introducing himself as a deputy akim of the Karaganda Region, he requested the director to help a third–year student at the college to pass a retake examination in Anatomy course. Based on this fact, criminal case was opened and sent to court for «unwarranted appropriation of title of representative of authority or civil servant, holding responsible state position, linked with commission of a crime on this basis» under the Part 2 of Article 390 of the Criminal Code of Kazakhstan» [3].

The crime was committed using a cell phone, and the network provider's software that monitors the cell phone signals can be used for the investigation. To confirm the occurrence of the conversation the information from the provider is used, which is given in a digital format.

The number of cases in which prosecutors, defenders, judges and other participating bodies encounter such «digital information» is continually increasing.

There are many definitions of «computer information» and «digital information» in the literature, and they have a lot in common.

For example, according to Zhempiisov, «computer information is an information that is stored on a computer media (hard disk drive and external media, such as flash drive, floppy disk, magneto–optical drive and optical disk drive), which can be transmitted through computer communication channels and manipulated only using a computer» [4, p. 184]. As the development of IT–technology indicates, the relevance of such definition is out of date. This is due to the emergence of new types of media (e.g. ID, SIM cards) and hardware (e.g., quantum computers) to obtain this information. However, we agree with the author's opinion that such information can be manipulated only with the help of computers.

Zigura argues that computer information includes data present in electronic–digital form on a medium, as well as the commands (programs) in computers or computer systems [5, 8 p.]. Such a definition is very broad and featureless. In our opinion, this is appropriate, because the number of types of computers is continuously growing. However, the author uses the concept of «electronic–digital form», which assumes that computer information is still transmitted digitally.

According to Zazulin, «digital information is an information encoded in a binary digital system, transmitted by any physical signal, which is not directly perceived by humans and stored on certain physical media – digital media specifically designed for its storage» [6, p. 20]. In his essay, Zazulin suggests using the term «digital information» in criminal proceedings. We support this suggestion. However, Zazulin does not discuss the essence of «digital information». He leaves the question of how it occurs open.

In addition, the concept of «digital evidence» is used in the United States. For example, according to Jackson et al, «digital evidence is information stored or transmitted in binary form that can be trusted in a court» [7]. It is incorrect to use this term because the evidence cannot be digital. Digital is the information, presented in binary form, on which the evidence is based.

In his thesis, Shanmugam describes digital forensics as a branch of science that deals with digital information produced, insured and transmitted by these computers in every investigation and trial [8, p. 11].

The concept is also found in the regulations of other foreign countries. For example, according to the Convention on Cybercrime of the Council of Europe, «computer data» means any fact, information or concept presented in a form suitable for processing in a computer system, including programs that control functions of a computer system [9]. But at the same time, it describes the introduction of digital technologies as one of the reasons for signing the Convention. This confuses whether the information should be called «digital information» or «computer information».

For further analysis, we will look in more detail at what «digital information» is, its units of measurement, the principles of encoding and transmitting.

Information (informatio) in Latin means data, explanation and presentation. Information is classified differently, in accordance with different systems of concepts in each science. In philosophy, information is divided into objective and subjective. Objective information reflects the phenomena of nature and human society. Subjective information is created by people and reflects their views on objective phenomena.

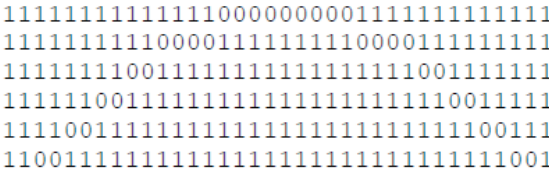
In computer science, analog information and digital information are considered separately. Analog information is information that is recognized by the human senses (color, sound, heat, taste, smell, etc.). If you mark different colors with numbers and sounds with different notes, you can digitalize analog information. For example, music is transmitted as analog information, but if you record it with notes, it becomes digital.

The process of converting a message to a combination of characters is called coding. The sequence of two characters is called a binary code. This means that the information can be represented by two characters. Computer recognizes two states: presence of a signal (i.e. voltage or current) or absence of a signal (i.e. no voltage or current). These two states are encoded in the form of numbers 1 and 0.

A binary number 0 or 1 is called a bit. Bit is a unit of measurement of information. Thus, any information can be measured in bits.

The whole concept is clarified in the illustration (Fig. 1).

Sample image



Sample image in digital format

Thus, in our opinion, the term «digital information» should be interpreted as information created, received, transmitted and stored by computers, and should be used in criminal proceedings instead of «computer information».

Based on the analysis, we offer an interpretation of digital information as follows: «digital information is information created, received, stored and transmitted by computers through coding into binary format».

At the same time, there is no consistency in the use of the concept of «computer information», as it is not clearly defined in the Law and the Code of Criminal Procedure of Kazakhstan.

In accordance with the Paragraph b) of Article 3 of the decree of the President of the Republic of Kazakhstan «on ratification of the agreement on cooperation of the member states of the Commonwealth of Independent States in combating crime in the field of computer information» from June 25, 2002, computer information is information stored in a computer's storage, including information transmitted on machines or other carriers, or through communication channels in a form accessible to computers.

Resolution No.599 of the Government of the Republic of Kazakhstan «on submission of a proposal to the President of the Republic of Kazakhstan to sign an agreement on cooperation of the Commonwealth of Independent States in combating crimes in the field of information technology» from September 28, 2018, states that computer information is information stored in the memory of a computer system, including information transmitted on a machine or other media, or through communication channels in a form accessible to computer systems.

The basic Law regulating public relations in the field of informatization, information and communication technologies does not have a clear definition of this concept. There is only a similar definition: «electronic information resources is information in electronic and digital form contained in electronic media and objects of informatization».

However, this concept does not reveal the essence of digital information.

In accordance with Article 118 of the Code of Criminal Procedure of the Republic of Kazakhstan, money, valuables, property, objects, documents are recognized as physical evidence in ruling a criminal offense, in determining the facts of a case, in determining the guiltiness of a suspect or in determining the liability to mitigation of penalty.

In accordance with Article 120 of the Code of Criminal Procedure, documents are explanatory letters, acts of inventory, acts of audit, certificates, acts of tax audits, conclusions of tax authorities, as well as materials containing computer information, photographs, films, audio recordings and video recordings, which are received, requested or submitted in the manner prescribed by Article 122 of the Code of Criminal Procedure.

The Paragraph 41) of Article 3 of the Criminal Code of the Republic of Kazakhstan provides describes «electronic carrier as a physical carrier used for the storage of information in electronic form, as well as its recording or replaying with the help of technical devices».

According to this concept, an electronic carrier is a means of transmitting not only computer information, but also any information in electronic form.

Thus, in accordance with the ruling of the laws of the Republic of Kazakhstan, the digital information recorded on physical media, i.e. hard disk drives, flash drives, and others, containing exact information with regards to illegal actions can be considered as a physical evidence in criminal cases.

Based on the analysis, we propose to provide a legislative interpretation by introducing the concept of «digital information» in «On Informatization» Law of the Republic of Kazakhstan.

On the basis of the legal interpretation, we suggest replacing the words «computer information» in the Code of Criminal Procedure with the words «digital information», as well as restructuring the Part 3 of Article 120 of the Criminal Procedure Code as: «Documents may include data registered in written form, as well as other forms. In addition, documents include explanatory letters, acts of inventory, acts of audit, certificates, acts of tax audits, conclusions of tax authorities, as well as materials containing digital information, photos, films, audio recordings and video recordings, which are received, requested or submitted in the manner prescribed by Article 122 of this Code».

These recommendations are based on the analysis of international practice, and they help to bring the concept of «digital information» in line with the concepts in the government program «Digital Kazakhstan» and other official documents.

Список использованных источников:

1. Кримінальний кодекс України: Відомості Верховної Ради України от 05.04.2001 г. № 25–26. [Электронный ресурс] – Режим доступа: https://zakon.rada.gov.ua/laws/show/2341–14?lang=ru#Text (дата обращения: 20.01.2021).
2. О зарегистрированных уголовных правонарушениях: Форма отчета № 1–М. [Электронный ресурс] – Режим доступа: https://qamqor.gov.kz/portal/page/portal/POPageGroup/Services/Pravstat (дата обращения: 25.01.2021).
3. Банк судебных актов Верховного суда Республики Казахстан. [Элетронный ресурс] – Режим доступа: https://office.sud.kz/courtActs/index.xhtml (дата обращения: 25.01.2021).
4. Жемпиисов, Н.Ш. Комментарий к статьям Уголовного кодекса Республики Казахстан по преступлениям, отнесенным к подследственности финансовой полиции. /Н.Ш. Жемпиисов/ Астана: Полиграф – Мир, 2006. – 252 с.
5. Зигура, Н.А. Компьютерная информация как вид доказательств в уголовном процессе России. /Н.А. Зигура/ дис… канд. юрид. наук. – Челябинск, 2010. – 234 с.
6. Зайзулин, А.И. Правовые и Методологические основы использования цифровой информации в доказывании по уголовному делу. /А.И. Зайзулин/ дис… канд. юрид. наук. – Екатеринбург, 2018. – 234 с.
7. Goodison, S.E. Digital Evidence and the U.S. /S.E. Goodison, R.C. Davis, B.A. Jackson/ Criminal Justice System. Criminal Justice needs initiative. 2 (2015) – P. 1.
8. Shanmugam, K. Validating digital forensic evidence. /K. Shanmugam/ A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy – Brunel, 2011. – 203 p.
9. Convention on cybercrime: Budapest, 23.XI.2001. [Electronic resource] – Access mode: https://rm.coe.int/1680081561 (Access date: 29.01.2021).

List of References:

1. Kriminal'nij kodeks Ukraïni: Vidomosti Verhovnoï Radi Ukraïni ot 05.04.2001 g. № 25–26. [Jelektronnyj resurs] – Rezhim dostupa: https://zakon.rada.gov.ua/laws/show/2341–14?lang=ru#Text (data obrashhenija: 20.01.2021).
2. O zaregistrirovannyh ugolovnyh pravonarushenijah: Forma otcheta № 1–M. [Jelektronnyj resurs] – Rezhim dostupa: https://qamqor.gov.kz/portal/page/portal/POPageGroup/Services/Pravstat (data obrashhenija: 25.01.2021).
3. Bank sudebnyh aktov Verhovnogo suda Respubliki Kazahstan. [Jeletronnyj resurs] – Rezhim dostupa: https://office.sud.kz/courtActs/index.xhtml (data obrashhenija: 25.01.2021).
4. Zhempiisov, N.Sh. Kommentarij k stat'jam Ugolovnogo kodeksa Respubliki Kazahstan po prestuplenijam, otnesennym k podsledstvennosti finansovoj policii. /N.Sh. Zhempiisov/ Astana: Poligraf – Mir, 2006. – 252 s.
5. Zigura, N.A. Komp'juternaja informacija kak vid dokazatel'stv v ugolovnom processe Rossii. /N.A. Zigura/ dis… kand. jurid. nauk. – Cheljabinsk, 2010. – 234 s.
6. Zajzulin, A.I. Pravovye i Metodologicheskie osnovy ispol'zovanija cifrovoj informacii v dokazyvanii po ugolovnomu delu. /A.I. Zajzulin/ dis… kand. jurid. nauk. – Ekaterinburg, 2018. – 234 s.
7. Goodison, S.E. Digital Evidence and the U.S. /S.E. Goodison, R.C. Davis, B.A. Jackson/ Criminal Justice System. Criminal Justice needs initiative. 2 (2015) – R. 1.
8. Shanmugam, K. Validating digital forensic evidence. /K. Shanmugam/ A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy – Brunel, 2011. – 203 p.
9. Convention on cybercrime: Budapest, 23.XI.2001. [Electronic resource] – Access mode: https://rm.coe.int/1680081561 (Access date: 29.01.2021).