УДК 004.4

Цифровые технологии в расследовании преступлений

Елизавета Андреевна Пермякова[1], Александра Георгиевна Ковалева[2]

[1, 2] Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, Екатеринбург, Россия

[1] lzvtpermyakova@gmail.com

[2] AG.Kovaleva@urfu.ru

Аннотация. Правонарушения в финансовом секторе представляют угрозу экономической безопасности любой страны. Особое значение в деле борьбы с преступностью в исследуемой отрасли отводится компьютерной криминалистике, которая участвует в предупреждении и расследовании киберпреступлений. Так, в статье рассматриваются возможные направления в применении информационных технологий и специальная криминалистическая техника при расследовании преступлений.

Ключевые слова: цифровые технологии, большие данные, технологии дополненной реальности, технологии искусственного интеллекта, компьютерная криминалистика.

Digital Technologies in the Investigations of Crimes

Elizaveta A. Permyakova[1], Alexandra G. Kovaleva[2]

[1, 2] Ural Federal University named after the First President of Russia B. N. Yeltsin, Ekaterinburg, Russia

[1] lzvtpermyakova@gmail.com

[2] AG.Kovaleva@urfu.ru

Annotation. Financial offenses are threats to the economic security of any country. Particular importance in the duel against crime in the industry under the study is given to computer forensics, which is involved in the prevention and investigation of cybercrime. Thus, the article discusses possible directions in the application of information technology and special forensic techniques in the investigation of crimes.

Key words: digital technologies, big data, augmented reality technologies, artificial intelligence technology, computer forensics.

Nowadays, digital technologies are actively used to commit various crimes, ranging from the sale of drugs, embezzlement of funds in credit institutions, up to encroachments on human life and the security of the state. However, digital technologies may help in organizing the detection and investigation of crimes. So, the development of technologies and the introduction of the achievements of scientific and technological progress into the mechanism of committing modern crimes determines the need of improving the quality of scientific-methodological and technical-forensics support in the investigation of crimes, one of the priority areas of which is the use of various forensic techniques.

The purpose of this paper is to study the peculiarities of the use of special forensic techniques for extracting forensically significant information from cellular communications, analysis of technical means intended to detect cellular communications.

In the first half of 2021, 1.2 million crimes were registered in the Russian Federation, more than a quarter of them, 26.6%, are cybercrimes. Of the number of cybercrimes, 212.8 thousand were committed using the Internet, 126.7 thousand - mobile communications, 103.7 thousand - bank cards, 21.8 thousand - computer equipment, 6.6 thousand - software, 922 - spurious electronic payments. This adds up to 0.47 million. It is reported that pensioners became victims of cybercrimes in almost 40 thousand cases. In another 3.3 thousand cases- minors, in 1.4 thousand cases - invalids of I and II groups. In Russia, in 2021, the amount of damage caused only from remote (telephone) frauds is 45 billion rubles, the total damage from cybercrime is estimated at around 90 billion rubles. For comparison, in 2020 the damage from cybercrimes was estimated at around 70 billion rubles. According to the estimates of international expert communities, the damage from committed cybercrimes will increase annually, and in 2025 it will reach 10.5 trillion US dollars per year.

In terms of the development of forensic activities, it is possible to point out some potential opportunities for the use of digital technologies.

Technology of "big data" (synonyms - supermassive data, BIG DATA) provides new opportunities for the implementation of analytics, but hidden dependencies and search questions and answers based on the analysis of all heterogeneous data. As for Russia, in the system of the Ministry of Internal Affairs there are huge amounts of data, including those that are not systematized. Thus, information that is significant for analytics in the materials of criminal cases is currently processed by a machine. In the investigation of crimes, “big data” can be used to predict the commission of crimes in the future, put forward versions, plan a criminal investigation, and search for suspects and accused who have escaped from the investigation and trial [3].

In addition, the use of augmented reality technologies is no longer new in the criminalistics activities of various countries, where video cameras with 3D panoramic video recording are used in the inspection of the scene of the incident. For example, in the United States, technologies are already used to transfer the appearance of various crime scenes into the virtual world. When considering a case, judges virtually immerse themselves into the scene of the crime with the help of reality glasses.

Artificial intelligence technology may be applied in automated online assistants to investigators (interrogators) in the investigation of criminal cases. Thus, an online assistant (Alice technology in Yandex, Siri in Google) may easily carry out a standard interrogator, a witness when committing a type of crime. Moreover, such interrogation, with appropriate identification of the person, may potentially be carried out via remote access.

At present, one of the technical means used by criminals in encroachments is mobile cellular phones, with the help of which the criminal actions of the perpetrators are coordinated, threats and demands of the criminals are presented, the actions of accomplices in the preparation and concealment of criminal activity are determined [4].

Modern capabilities of mobile communications allow not only making calls and exchanging messages via cellular communication, but also using Internet technologies of various software tools (Telegram, WhatsApp, Skype, etc.) and social networks (VKontakte, Odnoklassniki, Facebook, etc.).

The use of special knowledge in the course of investigating crimes allows not only to identify and fix the traces of criminal activity left with the help of mobile cellular communications, but also to establish the location of the criminal or the victim he has kidnapped, to determine the route of their movement, to restore text and multimedia information transmitted using mobile device and find out whether the transmitted data belongs to a specific person. Modern provision of investigation subjects with special forensic equipment allows extracting complete information, including deleted information, from the contents and memory of mobile devices, electronic storage devices, SIM cards, recording devices, etc. at any stage of the investigation, including preliminary [2]. The most common among the subjects of the investigation were such types of special forensic techniques as: a universal device for extracting forensic information (UFED - UniversalForen sicExtractionDevice), a mobile forensic expert, XRY, MOBILedit, Tarantula, etc.).

The capabilities of a series of universal devices for extracting forensic information (UFED), the effectiveness of which is confirmed by the forensic and investigative practice of investigating crimes is of great importance. UFED TouchUltimate software allows getting information about the phone (IMEI / ESN); SIM card (ICCID and IMSI); dates, time, duration of calls, including deleted ones; directed SMS, MMS and voice messages and photo-media files transmitted via them, including deleted ones; phonebook entries, etc. The universal forensic data retrieval device allows extracting and restoring data from the Internet software installed on the seizure of mobile devices: chat messages and e-mail; images; video and audio files; determining the location of criminals or victims at a specific time and date; establishing routes of movement; cracking passwords of call logs, text messages, contacts in e-mail.

A significant advantage of the analyzed software package is the ability to recover data in instant messengers that have become widespread in Russia and abroad - instant messaging systems (Telegram, WhatsApp, Viber, etc.), as well as correspondence in various social networks (VKontakte, Odnoklassniki, Twitter, Facebook, etc.) [1].

Application the capabilities of special forensic techniques at the preliminary and initial stages of the investigation makes it possible to establish the location and routes of movement of the participants in the proceedings, to reveal the involvement of individuals in criminal encroachments, and at the subsequent stage of the investigation - to directly expose the perpetrators of the investigated encroachments and facilitate the comprehensive establishment of the circumstances of the criminal case [5].

To sum up, digital technologies in the near future are not able to completely replace the mental work of investigators, interrogators, prosecutors and judges.

Digital technologies should be aimed at reducing the time spent on the same type of operations performed in the activities of the investigator (interrogator), subject to the exclusion of the need to perform the same actions in the traditional way.

The financial costs of the development of digital technologies should be comparable to the economic effect of their implementation. The introduction of digital technologies in forensic activities should be accompanied by pilot projects, legal experiments in certain regions.

References

1. Yermakov S.V. Vozmozhnyye napravleniya ispol'zovaniya tsifrovykh tekhnologiy pri rassledovanii prestupleniy. // Kriminalistika v usloviyakh razvitiya informatsionnogo obshchestva (59-ye yezhegodnyye kriminalisticheskiye chteniya). / Tekst elektronnyy. – 2018

2. Kalyuzhny A.N. Nekotoryye aspekty primeneniya spetsial'noy kriminalisticheskoy tekhniki v raskrytii prestupleni. // Kriminalistika v usloviyakh razvitiya informatsionnogo obshchestva (59-ye yezhegodnyye kriminalisticheskiye chteniya). / Tekst elektronnyy. – 2018

3. Regulation of the Bank of Russia No. 375-P (2012) "Requirements to the Internal Control Rules of the Financial Institution for the Purposes of Counteraction to Legalization (Laundering) of Criminal Proceeds and Financing of Terrorism" (with amendments and supplement). // Tekst elektronnyy. – 2 March, 2012

4. The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption. // Wolfsberg FAQs on Risk Assessments for ML, Sanctions and Bribery & Corruption. / Tekst elektronnyy. – 2015

5. Zhubrin R.V. Combating money laundering (foreign and Russian experience). // Tekst elektronnyy. – 2018

Информация об авторах

Елизавета Андреевна Пермякова – студентка института радиоэлектроники и информационных технологий Уральского федерального университета (Екатеринбург, Россия). E-mail: lzvtpermyakova@gmail.com, https://orcid.org/0000-0003-2943-9159

Александра Георгиевна Ковалева – кандидат педагогических наук, доцент кафедры иностранных языков и перевода Уральского гуманитарного института Уральского федерального университета (Екатеринбург, Россия). E-mail: AG.Kovaleva@urfu.ru, https://orcid.org/0000-0002-9066-6783