Advances in Social Science, Education and Humanities Research, volume 441
6th International Conference on Social, economic, and academic leadership (ICSEAL-6-2019)

Leading Forensic and Sociological Aspects in Investigating Computer Crimes

Nina Olinder*
Toliatti state University
Belorysskaya str. 14, 445020 Toliatti
Russian Federation
e-mail: olindernv@yandex.ru

Aleksej Tsvetkov
Independent Legal Expert
Vyazovaya str. 10, 461010 Orenburg
Russian Federation
e-mail: tsvetcov42@mail.ru

Abstract Our paper discusses the leading features of the formation and functioning of a criminal group when committing crimes with the help of electronic payment systems. Currently, there is an increase in the number of computer crimes around the world. According to the Prosecutor General of the Russian Federation, the number of crimes in the IT sphere has increased. The most common are illegal access to computer information and malicious computer programs. At the same time, the number of investigated crimes is reduced. Most of these crimes, due to their technological complexity, are committed by organized groups that have their own internal connections, features, hierarchy, motives. This paper scrutinizes by what methods, methods and means these groups (members of groups, relations between them, social roles, etc.) can be investigated to build practical recommendations for law enforcement agencies to identify such groups and curb their activities. Our comparative analysis revealed the general characteristics of such groups, both in sociological theory and in criminology. Based on our own observations and analysis, it was concluded that an organized criminal group, being an independent category, and considered as an element of the forensic characteristics in forensics, meets all the characteristics of the group as a sociological phenomenon. Consequently, the methods of sociology can be used in two ways: first, to identify such groups, and second, to identify relationships and roles within groups in identifying and investigating computer crimes.

Keywords: *forensics, sociology, crime investigation, leadership, computer crimes*

1 Introduction

Every year, the number of computer crimes worldwide is growing. The number of unsolved crimes using high technologies in 2017 increased from 65949 to 90587 (an increase of 30.5%), and in 2018 amounted to 121247 crimes (+ 26%) (see Prosecutor General's Office 2019a; Prosecutor General's Office 2019b). In 2018, a tenfold increase in cybercrime over the past six years was noted: in 2013 - 11,000, in 2014 - 44,000; in 2016 - 66,000 crimes. The share of crimes under consideration of the total number of recorded crimes is 4.4% - this is almost every 20 crime (Prosecutor General's Office 2019a).

In the first half of 2018, only fraudulent acts committed using electronic means of payment (Article 159.3 of the Criminal Code of the Russian Federation) increased 7 times. Russian telecommunication company Rostelecom noted that at the end of 2018, the number of cyber-attacks in the Russian Federation doubled. Hackers' revenues reached 2 billion rubles. in 2018, specialists registered 765,259 attacks, which is 89% more than in 2017 (27% of attacks were successful). The victims of 75% of cybercriminals were mainly financial institutions, as well as companies working in the field of electronic commerce and the gaming business. The situation on the world stage is similar. Thus, according to the official website of the Ministry of Internal Affairs of the Republic of Belarus, the number of crimes in the field of high technologies in 2018 increased by 53% compared to 2017 (from 3099 to 4741 crimes) (Ministry of Internal Affairs of the Republic of Belarus 2019). According to the report of the international company Group-IB, specializing in the prevention of cyber attacks, the top 3 countries of the most active pro-government hiker groups include China, North Korea and Iran.

The most dangerous threats in the world are financial institutions (banks); on average, a successful attack of 1-2 banks takes place every month, the average damage from the attack is 132 million rubles. ($ 2 million), in 2018 the number of attacks increased three times. Bank card fraud remains among the most dangerous threats to individuals (due, inter alia, to an underdeveloped behavioral analysis system during transactions) (Group-IB 2018).

In addition to the increase in the crimes under consideration, the methods of their commission become more complicated, the crimes become more "technically thought out" which is confirmed by data on a decrease in the disclosure of these crimes.

This paper conducted a study of the composition and characteristics of organized groups that commit computer crimes. Further, the article identifies the signs and factors affecting the education (creation) of such social groups. In addition, the social roles of members of organized groups committing computer crimes, internal connections between them, and the features of "combining" intragroup roles were revealed. The article offers recommendations for practitioners to identify criminal groups, as well as recommendations for determining the roles of each participant and the relationships between them.

2. Literature review

Every study aimed at identifying the identity of the offender is a complex task that occupies a special place in the forensic characterization. The identity of the criminal is studied in many legal sciences: criminal law, criminology, forensic science, legal psychology, as well as in other, non-legal sciences: psychology, sociology, etc. As noted by Kasatkin (1997), 41% of investigators and 38% of judges note the importance of investigating the identity of criminals committing computer crimes, since according to these cases the model of behavior of the offender and his circle of interests are very specific (Kasatkin 1997). It is known that every criminal is considered as a person: i.e. his views, value orientations, interests, psychological characteristics, but his position and attitude to society is of even greater importance. It is this question that interested the authors of this article: "How does the forensic and sociological characteristics of the personality of the criminal and the criminal group intersect?" The study of the identity of the criminal and his criminal behavior affects both the identification of the method of committing a crime, the circumstances that contributed to its commission, and the objective investigation. Among the basic characteristics of a criminal's personality, it is customary to single out: socio-demographic (external side), moral and psychological characteristics (internal side). Since the considered category of crimes, as a rule, is committed by a group of persons (due to its technological complexity), it is relevant not only to study the identity of the criminal, but in relation to the criminal group.

It should be noted that the study of such a multifaceted phenomenon as a person indicates that this category is of interest to many sciences because its analysis can be carried out in specific aspects. So, the problem of personality in sociology is the question of what place a person occupies in social communities. Sociology of personality as a special sociological theory appeared on the verge of the XIX - XX centuries. Its founders are Linton (1949), Sorokin (1992), Moreno (1994), Cooley (2000), or Mead (2009).

Prominent forensic scientists studied the identity of the criminal in forensics: Glazyrin (1975), Vedernikov (1984), Belkin (2001), Ahmedshin (2006) and others. The issues of the activity of criminal groups in forensics were studied by Kulikov (1994), Yablokov (2002), and others. Vekhov (1994, pp. 45-51), who was one of the first to offer their classification, paid attention to the study of the identity of criminals and criminal groups in constructing the forensic characteristics of computer crimes. Melekhin and Alembekov (2009), who proposed a classification of criminals committing crimes involving the use of plastic cards Meshcheryakov (2001) and others. Osi This question is also of interest to foreign authors. The work of Katz et al. (1963), Ponemon Institute (2015), Ipsos MORI (2016); Grobler and Louwrens (2007) and others.

The main objective of this paper is an interdisciplinary analysis of criminal groups committing computer crimes. To achieve this goal, the following tasks were solved: the features of the formation and functioning of criminal groups committing computer crimes were identified; analyzed the roles of members of the criminal group, and from the relationship; identified factors affecting the viability of the criminal group, and also proposed practical recommendations on identifying such groups and curbing their activities for law enforcement agencies.

3. Research methods

In the course of the study, both general scientific and especially legal and sociological methods were applied. The main general scientific method was analysis, which made it possible to comprehensively study the characteristics of the criminal group as a whole, and its individual members; develop a classification of members of a criminal group committing computer crimes.

As a result of using this method, the hypothesis about the possibility of a criminalistic study of a criminal group, including using sociological research methods, has been confirmed. Based on the formal legal method, an analysis was made of the criminalistic characteristics of the criminal group and the identity of the offender in it, a conclusion was drawn on the motives for joining the group.

The comparative method allowed us to assess the relationship between sociological and forensic approaches to the study of the identity of a criminal group. Consequently, the main factors affecting the formation of such groups, as well as the types of groups, were identified.

The method of observation and interviewing allowed us to collect empirical material - interviews of investigators, interrogators and security officers regarding members of a criminal group, their relations with specialized services, their special knowledge and skills, etc.

4. Results and discussion

Forensics is closely associated with many disciplines of a non-legal profile, and in particular with psychology and sociology. This is especially pronounced in the fact that forensics is aimed at investigative and judicial activities, which have a pronounced social side, and in particular, in the forensic study of personality, sociological data are used. In the sociology of personality as a characteristic of the latter, the most interesting are the problems of the social roles of the individual, as well as the formation of microgroups, social and psychological characteristics of age groups (Konovalova 1980, pp. 15-16).

This study was the first to conduct an interdisciplinary analysis of a computer crime group. Computer crimes, due to their characteristics, are usually committed by groups. For a deeper study of the processes of formation and activities of such groups, it is advisable to consider them not only from the point of view of the forensic characteristics, but also using sociological research methods. In the sociology of management, it is customary to single out factors of group behavior and group efficiency (constants and variables). This information can help the investigator in understanding and predicting the behavior of members of the criminal group, and, therefore, help in the investigation of computer crimes. So, among the main constant factors in the formation and operation of a criminal group committing computer crimes can be distinguished (Kartashova et al. 2001):

- Professional harmony of the group - quite often members of the group are “selected” on closed hacker sites, before becoming a member of such a group a person must show his professionalism in the field of computer technology, skills in computer technology and programs, i.e. The basis for joining the group is, inter alia, professional suitability. Within a group, as a rule, roles are distributed, but if necessary, the role of one shuttle of a group can be performed by another. An objective pattern can be traced in the category of cases under consideration: the more sophisticated and technically more complex the crime, the fewer people are able to ensure the implementation of its individual “high-tech” stages. Moreover, situations often arise when only one way of committing a crime or the used tool (tool) can almost unambiguously indicate the person who committed it (Meshcheryakov 2001). In addition, there is a tendency to conceal new crime technologies even from persons who were previously members of a temporarily established criminal group. As a result of this, the fact of the outwardly unfounded, temporarily increased anonymity of a certain person or group of persons at a specialized forum, a noticeable decrease, in comparison with previous periods, of information about current and planned criminal actions coming from him or them to other forum participants, together with other information, may testify that the next criminal group has been created and is functioning that implements a new, previously unknown crime technology of the category in question;
- Moral and psychological cohesion of the group — a feature of such groups is that on the one hand its members are “as if impersonal” - they act under “nicknames”, often their real names are unknown, on the other, a hacker with his name (“nickname”) is known among the "party" of other hackers. Of great importance is his authority as a specialist. Among the members of the group are common interests, which strengthens the moral and psychological connection between them;
- Interpersonal compatibility - this factor is the most significant, since the integrity of the group directly depends on “comfort”. A feature of such groups is that people who are different in temperament, character and style of behavior gather in it. In such groups, along with “closed” people (with elements of autism) who are engaged only in computer programs, they may not communicate with other people, there are people who, for example, are engaged in cashing out money, and these are people with an “open” character. Thus, interpersonal compatibility is built on remote access, and sometimes people interact who in reality could never have interacted;
- Purposefulness and democracy - this factor depends directly on the leaders of the group, as a rule, all members of the group are ambitious, have special knowledge and skills, consider themselves superior to others, can use technology in their criminal activities, and often consider themselves to be white-collar crime. In such groups, as a rule, a high level of democracy, sometimes unnecessarily demonstrated, it is very difficult to establish leadership roles in the investigation and determine the leader;
- Productivity of the group depends on the study of all elements of the attack, the chain of actions from theft to the withdrawal of money, a clear distribution of roles.

Among the variable factors can be identified:

- group level of claims - this factor may vary depending on the criminal intent. When making one attack, members of the group can determine the claims in equal volume, and with another, distribute in proportion to the “contribution” of each;
- qualifications of the members of the criminal group and the position in the group - affects the roles they perform, with the growth of qualifications a person can “move” from one role to another. Moreover, with the acquisition of experience, the number of roles that one member of the group can fulfill increases. At some point, this can lead to a numerical reduction of the group, but to a complication of attacks, and therefore an increase in the amount of criminal attacks;
- requirements for the final result - since in such groups there is a clear distribution of roles (which will be discussed later), the final result for each group member will be precisely its stage. Features of the functioning of such groups that sometimes part of the group members may be “random”, hired “blindly”, and not know about the presence of other members;
- degree of interaction with other members of the group; intra-group interpersonal communication and the constancy or temporary nature of the group.

It seems to us important to combine these three factors, since they are closely interconnected precisely in this category of groups. Two types of groups can be distinguished: permanent - long-formed, worked-up groups. As a rule, such groups are overgrown with legends, it is their actions that are discussed in closed specialized forums, sometimes it is not entirely clear whether this is a real group or a phantom group. For example, so far there is no exact information about the person who created Bitcoin: there are three versions: this is a specific person, this is a group of people, and this is a fictional character. In such groups, a clear interaction between individual members is set up, all chains of the group are stable. The second type of groups are groups created spontaneously, sometimes to perform a specific task (for example, to develop a virus program). These groups are temporary, members of the group can not only not know each other, but also not assume the presence of each other. Another feature of the characteristic of this factor is that intra-group communication takes place in forums, in closed groups, group members know each other by nicknames and avatars, and in real life they may never intersect at all.

In the mid-1990s, the first studies were conducted, during which the age of the "computer" criminals was determined. 54% of criminals were 20–40 years old, 33% had no more than 20 years of age at the time the crime was committed, 13% were older than 40 years. Most (83%) were men, but there was a rapid increase in the proportion of women. At the end of the 1990s, at the first international conference on computer security, Interpol announced similar averaged data for this category of people: three groups were identified, namely 11-15 years old, 17-25 years old and 30-45 years old (Vekhov 1995, pp. 50-52). Similar data are provided by Meshcheryakov (2001), who at the same time considers it advisable to distinguish only two groups of persons from the forensic point of view: the first group of 13-20 years old, the second from 21 years onwards (see Meshcheryakov 2001). schoolchildren and students who are mainly involved in petty theft and fraud, while the second group is represented by individuals with high professional skills, they commit acts are deliberate self-serving character.

Interesting data was published by Osipenko (2009, p. 213) - 96% of network crimes are committed by males of 14 to 25 years old. In this group young people aged 19-20 years predominate. He noted that the distribution of persons who commit computer crimes by age group does not seem sufficiently informative, and in most cases age does not play a decisive role in the forensic sense. However, one cannot agree with this, since some roles require training, and sometimes having one's own income, which, for example, may not be with a teenager or a young man. With regard to gender, our analysis of criminal cases shows that in most cases the criminals are men. This is determined by such factors as the circle of preferential communication and the interests of people in this circle (a girl who is interested in computer technology is forced to communicate mainly with girls who are not interested in the professional aspects of computer technology); the amount of free time and its structure (for women, due to the increased workload of household chores, there is significantly less free time for self-education and communication according to professional interests) and other factors.

Of particular importance from the point of view of forensics, and from the point of view of the sociological approach is the distribution of social roles in the group. Earlier, by conducting a forensic analysis of the identity of the criminal who committed the crime, using electronic means of payment and systems, the author proposed the following classification of members of the criminal group (Olinder et al. 2019). “Analyst” - a person who studies electronic payment systems, identifying the strengths and weaknesses of each, and based on the information received develops a technology for committing a crime. "Programmer" - a person who, by order of "analytics", develops software for the implementation of the latest technology for committing a crime. “Tester” - a person who verifies in practice, using the developed software tools, the technology for committing a crime as a whole or its individual elements. “Technology user” - a person who has purchased the technology for committing a crime as a whole or its individual elements; and which uses it for unlawful purposes, receives results (for example, details of access to an account in an electronic payment system stolen by a malicious program) for the purpose of reselling them to other persons. "Cashing Organizer" - a person who buys the results obtained from a "user of technology", allowing them to be directly used to withdraw funds from the electronic payment system. "Outcash" - a person

who withdraws (cash out) money from the payment system for the agreed percentage. Each of these roles is independent, but at the same time, can be combined with another role.

Based on the classification of criminal group roles given above and the classification of roles in the group according to the type of behavior “Behavior aimed at solving problems”, the following roles can be distinguished: “initiator-inspirer”, “analyst”, “programmer-developer”, “tester” ”,“ Technology user ”,“ controller-appraiser ”,“ recruiter ”. Table 1 that follows shows the results of a comparative analysis. All roles analyzed are professional, i.e. determined by the level of professional skill, based on the type of behavior "Behavior aimed at solving problems".

Table 1. Interdisciplinary analysis of social roles in a criminal group

Social role	Characterization of the role by type of behavior (sociology)	Forensic characteristics of a role in a criminal group
Initiator	A person who is a leader puts forward ideas of activity, sets a goal, takes part in the development of a program	The leader of the group, which determines the direction of criminal activity, determines the ultimate goal of the crime, works out the mechanism of hacker attack
Analyst	A person working not with people, but with information that is structured, grouped and analyzed. Based on the analysis, forecasts and conclusions can be made	Often, "analysts" are combined into groups that develop individual elements of such technology and coordinate their work during anonymous communication in closed from extraneous sections of the "carder" or "hacker" forums. Sells the results of his work for a predetermined amount or claims to be a percentage of the stolen money if he works as part of a stable criminal group
Software developer	Works out the ideas submitted by the initiator, deals with the setting of tasks and their solution	Develops a software product. Payment for the work of the "programmer" is carried out according to the principles set forth for payment for the work of the "analyst"
Tester	The person who should conduct experiments (possibly social) to introduce “new products”	The well-established principles of remuneration of the “tester” at the time of our writing are unknown. For potentially highly profitable technologies, the fact and content of the work of the “analyst”, “programmer”, “tester” is kept secret from their friends and the hacker-carder community, since subsequently such technology or its individual elements will become a sale
Technology user	The so-called "buyer" who for the money acquires the developed product as an end user or as a reseller	“Technology user” - a person who has purchased the technology for committing a crime as a whole or its individual elements; and which uses it for unlawful purposes, receives results (for example, details of access to an account stolen by a malicious program) for the purpose of reselling them to other persons
Appraiser	Critically evaluates the activities of the group at all stages of its activities, identifies deviations in order to coordinate tasks	A person who monitors the frequency of hacker attacks, reveals signs of exposure, is designed to ensure the safety of the group
Recruiter	A person with professional communication skills, possibly with a psychological background, who can understand and evaluate the motives and values of a hidden interlocutor	Acts as a picker of the necessary specialists in a criminal group

Source: Own results

As part of the study, an expert survey and questioning of investigators was conducted. The target sample was 25 people, according to the principle of participation in the investigation of such criminal cases. The aim of the study was to analyze the activities of criminal groups committing computer crimes based on sociological characteristics:

- Characteristics of group members - experience, abilities, education;
- Structural characteristics of the group - communications and norms; the status and roles of each participant; personal likes and dislikes; strength and conformism;
- Situational characteristic of the group - the size of the group; spatial arrangement of the group; tasks solved by the group; reward system.

Analyzing the results of the study, we can draw the following conclusions. Regarding the age and sex characteristics of members of criminal groups, it can be unequivocally stated that these are men, mainly aged 21 to 30 years. This is due to the fact that it is this age that is characterized by greater awareness in the field of modern computer and Internet technologies, which are able to get ahead of existing information protection technologies.

As for the level of education of persons who entered the criminal community in the category of cases under consideration, in most cases they are persons with higher or secondary vocational education. Moreover, the respondents answered that most members of the criminal group have special skills in the field of committed offenses. Could this mean that they have a specialized education, it's difficult to say, but the fact is clear that they are educated people who have knowledge in IT technologies, which can be assessed as "above average" level than most people in our country. In support of these words, let us turn our attention to the possible answers to the question: "Is it true that people included in the criminal community have experience in professional activities in the field of high technology?" Fully agreed with this statement 20% of respondents, and another 36% answered "rather yes than no."

Speaking about the structural characteristics of group members, the following should be noted. In intra-group communication, as a rule, closed groups are used in instant messengers (Viber, WhatsApp) and closed sites. One of the reasons for choosing potential members of a criminal group can be considered a demonstration of abilities on hacker sites and authority among the professional community in the field of high technology.

About 60% of the respondents said that in the criminal group committing computer crimes, there is a clear distribution of social roles. Moreover, investigators agree that in most cases, it can be argued that the classification proposed above reflects social roles in the criminal group, such as "initiator-inspirer", "analyst", "programmer-developer", "tester", "user of technology", "Controller appraiser." It should be noted that it is possible to combine several social roles with one member of the group. Moreover, the overwhelming majority of respondents (96%) agree with the statement that the status of a member of a criminal group depends on his social role.

The situational characteristic of the investigated criminal group is as follows. As a rule, this is a group that includes a small number of participants 3-5 people, in rare cases up to 3 people. Experts agree that such crimes are most often committed remotely. Moreover, as a rule, members of a criminal group are residents of different settlements. A little more than half of the respondents believe that at the time of the commission of illegal actions, the criminals are in Internet cafes or in other public places (for example, coworking centers).

It can clearly be argued that groups of people who commit computer crimes act for the purpose of profit. Within the group, for certain types of work (for example, writing a computer program), a fixed remuneration is provided. Moreover, the amount of remuneration received, as a rule, depends on the status of a member of a criminal group and on the significance of the role that he performs.

5. Conclusions

Thus, it is possible to draw conclusions about the common signs of a criminal group committing computer crimes, which may be useful to the investigator when planning the investigation of computer crimes in general, and when planning certain investigative actions.

Another criterion for determining the identity of the offender is the motive of the crime, since it is an element of the subjective side of the crime, and is considered as a factor inducing crimes in criminalistics and sociology. The main motives for joining a group in sociology are: achieving the goal; affiliate motive; security; communication needs; power strengthening. In criminal investigations, several classifications of the identity of computer criminals have been proposed, based on the motive of the crime. For example, Vekhov (1995) singled out the following motives underlying the classification of subjects of computer crimes that he developed: a demonstration of intellectual and professional abilities; obtaining material benefits as an accompanying other motive; computer phobias; selfish motive as the main (Vekhov 1995). The same motives act for entry into the criminal community.

Krylov (1998) highlighted similar motives underlying the classification of subjects of crimes in the field of computer information: satisfaction of one's own ambitions; achievement of political, military, economic goals; political impact; obtaining personal property and non-property benefits; obtaining satisfaction from destructive activities; elimination of the "computer" factor as a cause of anxiety (Krylov 1998, pp. 231-232).

Meshcheryakov (2001) gives the following motives for committing crimes in the field of computer information: revenge, gaining money, hooliganism and curiosity, professional self-affirmation (Meshcheryakov 2001; p. 27).

The main motive that characterizes the identity of the offender when committing crimes of this category is self-interest, that is, the desire to extract material or other property benefits from the crime or the intention to get rid of material costs. This motive brings together in a criminal group persons who, under any other circumstances, might not have begun to conduct joint activities. However, in addition to this, there are other motives that are

specific to computer crimes. We attributed such motives to raising the status in the criminal hierarchy and monetary or other material obligations.

Thus, we can make a general conclusion that the results of the study showed stable links between behavioral skills and roles in the criminal group. The specific roles of members of a criminal group in the commission of computer crimes are highlighted. Knowledge of the role and personality traits of the criminal will allow law enforcement officials to correctly and timely outline the circle of suspects in the investigation of crimes of this category, as well as to prevent the commission of computer crimes and identify potential participants in such criminal groups.

Acknowledgments

The authors would like to thank law enforcement officers, investigators, for the time taken to the questionnaire and answers to questions. The results of the work were presented at the international scientific-practical conference "Legal regulation of the digital economy: problems and development prospects."

References

Ahmedshin RL (2006) Forensic characteristics of the personality of a criminal. https://cyberleninka.ru/article/n/kriminalisticheskaya-harakteristika-lichnosti-prestupnika-priroda-i-soderzhanie Accessed 29 Mar 2020

Belkin RS, Forensics: the problems of today. Topical issues of Russian forensics, 1st edn. (Moscow, Norma, 2001), 240 p.

Cooley Ch, Human nature and social order, 1st edn. (Moscow: Idea-Press: House of Intellectual Books, 2000), 309 p.

Glazyrin VF, Investigation of the identity of the accused and tactics of investigative actions, 1st edn. (Sverdlovsk, 1975), 156 p.

Grobler C, Louwrens C (2007) Digital forensic readiness as a component of information security best practice, FIP International Information Security Conference, Vol. 232, Springer, Boston, MA, pp. 13-24. doi: 10.1007/978-0-387-72367-9_2

Group-IB (2018) Group-IB resented a report on cybercrime and encouraged the market to hight. https://www.group-ib.ru/media/hi-tech-crime-trends-2018 Accessed 12 Apr 2020

Ipsos MORI (2016) Cyber security breaches survey 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf

Kartashova LV, Nikonova TV, Solomanidina TO, Organizational Behavior: Textbook, 1st edn. (Moscow: INFRA-M, 2001), 220 p.

Kasatkin AV (1997) The tactics of collecting and using computer information in the investigation of crimes. http://www.dslib.net/kriminal-process/taktika-sobiranija-i-ispolzovanija-kompjuternoj-informacii-pri-rassledovanii.html Accessed 11 Apr 2020

Katz S, Ford AB, Moskowitz RW, Jackson BA, Jaffe MW (1963) Studies of illness in the aged: the index of ADL: a standardized measure of biological and psychosocial function. Jama 185(12):914-91927. doi: 10.1001/jama.1963.03060120024016

Konovalova VE (1980) Forensic tactics and sociology. Actual problems of Soviet forensics. All-Union Institute for the Study of Causes and the Development of Crime Prevention Measures, Moscow, pp.15-16.

Krylov VV, Investigation of information crimes, 1st edn. (Moscow: Gorodets, 1998), 264 p.

Kulikov VI, Fundamentals of the forensic theory of organized crime, 1st edn. (Ulyanovsk: Branch of Moscow State University, 1994), 256 p.

Linton R (1949) Problems of Status Personality. In: Sargent SS, Smith MW (eds.) Culture and personality, pp. 163–173. https://doi.org/10.1037/11254-010 Accessed 11 Mar 2020

Mead JG, Favorites, 1st edn. (Moscow, Publishing house of the RAS INION, 2009), 290 p.

Melekhin OY, Alembekov DR (2009) Crimes associated with the use of plastic means of payment. Citizen and Law 7:88-90

Meshcheryakov VA, Crimes in the field of computer information: legal and forensic analysis, 1st edn. (Voronezh: Voronezh State University, 2001), 176 p.

Ministry of Internal Affairs of the Republic of Belarus (2019) Statistics of URPSVT for 2018. Office for the Disclosure of Crimes in the Field of High Technologies (Office “K”). Official website of the Ministry of Internal Affairs of the Republic of Belarus. www.gov.by Accessed 10 Apr 2020

Moreno JAL (1994) Sociometry: An Experimental Method and the Science of Society, 1st edn. (Moscow: Progress; Univers, 1994), 352 p.

Olinder NV, Romanova VV, Tovysheva IZ, Yunoshev SV, Gambarova EA (2019) Special aspects of digital information acquisition on the Internet used in criminal investigations and personal data analysis. Amazonia Investiga 8(19):491-499.

Osipenko AL, Network Computer Crime: Theory and Practice of Fighting: Monograph, 1st edn. (Omsk: Omsk Academy of the Ministry of Internal Affairs of Russia, 2009), 213 p.

Ponemon Institute (2015) Global report on the cost of cybercrime. https://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states Accessed 11 Apr 2020

Prosecutor General's Office (2019a) The number of crimes in the IT sector has increased. https://roskomsvoboda.org/40924/ Accessed 19 Mar 2020

Prosecutor General's Office (2019b) Cybercrime is growing more actively than other types of criminal activities. https://habr.com/ru/news/t/469365 Accessed 19 Mar 2020

Sorokin PA, Man. Civilization. Society, 1st edn. (Moscow: Политиздат, 1992), 543 p.

Vedernikov TA, The identity of the criminal as an element of the forensic characteristics, 1st edn. (Moscow: Law Press, 1984), 230 p.

Vekhov VB (1995) Forensic characteristics and improvement of the practice of investigation and prevention of crimes committed using computer technology, Volgograd: VSSh the Ministry of Internal Affairs of Russia. http://lawtheses.com/kriminalisticheskaya-harakteristika-i-sovershenstvovanie-praktiki-rassledovaniya-i-preduprezhdeniya-prestupleniy-soversha Accessed 24 Mar 2020

Yablokov NP, Investigation of Organized Crime, 1st edn. (Moscow: Lawyer, 2002), 172 p.