MOTIVES AND OBJECTIVES OF CRIME COMMISSION AGAINST INFORMATION SECURITY

[a]ALEXANDRA YURYEVNA BOKOVNYA, [b]ILDAR RUSTAMOVICH BEGISHEV, [c]ALBINA ALEKSANDROVNA SHUTOVA, [d]DIANA DAVLETOVNA BERSEI, [e]ELENA ANATOLIEVNA PERSHINA, [f]VALERY PAVLOVICH POTUDINSKY

[a]Ph. D. in Law, Faculty of Law, Department of Criminal Law, Kazan Federal University, Kremlyovskaya St, 18, Kazan, Republic of Tatarstan, Russia
[b]Ph. D. in Law, Senior Researcher, Kazan Innovative University named after V.G. Timiryasov, 42 Moskovskaya str., Kazan, 420111, Russia
[c]Ph. D. in Law, Senior Researcher, Izhevsk Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia), Izhevsk, Russia (Russian Federation)
[d]Ph. D. in Law, Department of Legal and Special Disciplines, Stavropol branch of RANEPA, Stavropol, Russia (Russian Federation),
[e]Ph. D. in Law, Department of General Humanitarian and Legal Disciplines, Stavropol branch of the Moscow State Pedagogical University, Stavropol, Russia (Russian Federation)
[f]Ph. D. in Law, Department of Legal and Special Disciplines, Stavropol branch of RANEPA, Stavropol, Russia (Russian Federation),
e-mail: [a]kafedra.ksu@yandex.ru. [b]begishev@mail.ru. [c]shutova1993@inbox.ru. [d]bi.bersej2012@yandex.ru [e] pershina_geminus@mail.ru [f]valerypotud@yandex.ru

Abstract: The article discusses the motives and goals of committing crimes against information security. The authors conclude that the motive for crimes against information security is a deliberate motivation, through which the subject has the opportunity to satisfy his own needs via the commission of a crime. If you establish the motive, you can get the answer to the question why the crime was committed. The goal is the result image, which is important for the subject when the crime is committed. If the goal is set, then, accordingly, there is an answer to the question why the crime against information security was conceived and committed.

Keywords: motive, goal, crime, cybersecurity, information security, digital technology, information protection, cybercrime.

1 Introduction

In the modern age of digital technologies, information security becomes vital for all participants in legal relations. It accumulates the methods and means of information system protection, which includes the totality of information resources of citizens, companies and the state, as well as digital technologies and software and hardware systems.

In this regard, knowledge of ways to protect the information infrastructure from criminal encroachments becomes increasingly relevant (Begishev et al., 2019). Computer attacks (Begishev et al., 2019) and other information security incidents negatively affect the performance (Malik & Islam, 2019) and cybersecurity state (Khisamova et al., 2019) of any organization in the context of digital crimes (Bokovnya et al., 2019).

Digital technology is an integral part of our daily lives. Regardless of whether we have a computer at home, whether we use the opportunity to receive state and municipal services in digital form, or simply operate electronic gadgets, the dependence of society on technology increases. A secure digital environment enhances public confidence and contributes to a stable and prosperous state. Government and the business community are also leverage the power of the technological revolution through the wider adoption and application of digital technology. Traditional forms of crime have also evolved. Criminal associations begin to master the information and telecommunication network called Internet. Digital crime is developing at an incredibly fast pace; new types of criminal acts appear constantly. Therefore, we must keep up with digital technologies, understand the opportunities that they create for cybercriminals, and how they can be used as a tool to combat cybercrime (Begishev et al., 2020).

All this determined the importance of a comprehensive study of crime motives and goals against information security

2 Methods

The materials for the work were the provisions of the Russian criminal and information legislation, as well as regulatory legal actsin the field of information security.

The reliability of the obtained results is provided on the basis of the analysis of a significant and necessary array of legislative norms, statistical data, as well as the use of modern study methods of legal establishment: historical and legal, logical, formal, legal, comparative law, system-structural and other methods of scientific knowledge.

3 Results and discussion

There is a number of definitions of information security in the literature. In particular, according to T.A. Martirosyan information security is a state of security of an individual, society and state in the information sphere from possible internal and external threats (Martirosyan, 2005). According to V.D. Kurushin and V.A. Minaev, information security is a state of information environment security for society, ensuring its formation and development in the interests of citizens, organizations and the state (Kurushin & Minaev, 1998). A.V. Mnatsakanyan notes that information security is a constantly maintained and ensured state of information sphere protection in state interests, the interests of society and citizens (Mnatsakyan, 2014). Most fully, in our opinion, information security is determined by T.A. Polyakova: in her opinion, this is a state of RF national interest protection in the information sphere from internal and external threats. This sphere consists of a combination of balanced interests of an individual, society and the state, which corresponds to the principle of national security provision in the information sphere, as defined by the Strategy for the Development of the Information Society in Russian Federation (Polyakova, 2008).

V.A. Shepetko singles out the following goals of information security:

- prevention of information leakage, theft, loss, distortion, and falsification;
- prevention of threats to individual, society, and state security;
- prevention of unauthorized actions destroying modifications, distorting, copying, or blocking information;
- prevention of other forms of unlawful interference with information resources and information systems, ensuring the legal regime of documented information;
- protection of the constitutional rights of citizens to maintain personal secrets and confidentiality of personal data available in information systems;
- maintaining state secrets, confidentiality of documented information in accordance with the law;
- ensuring the rights of subjects in information processes and during the development, production and application of information systems, technologies and the means of their provision (Shepetko, 2016).

The encroachment on information security at all levels becomes global. Crimes committed in the area under consideration are of the most diverse nature and orientation.

Today, there is a number of classifications of crimes in the field of information security, sponsored by the experts of the United Nations Economic Development Organization, participants in the Conference of Lawyers in the USA, etc. However, the conceptual approach to the concept of “information security”, formulated in the Russian Federation Information Security

Doctrine, indicates the need for classification of crimes in the field of information security, taking into account Russian legal realities. For this reason, we agree with A.V. Mnatsakanyan, who identifies four groups of crimes in the field of information security: crimes against the interests of the state in the information sphere, crimes against the interests of an individual in the information sphere, crimes against the interests of society in the information sphere, as well as the crimes in the field of computer information, which are included in the Chapter 28 of RF Criminal Code (Mnatsakyan, 2014).

Given the above classification, motives and goals of crimes in the field of information security are of interest. The motive acts as a driving force in the process of committing a crime. According to M.P. Chubinsky, motive can be defined as “an internal force, which, generating a volitional process, moves an individual in his conscious activity and leads, with the help of his whole psyche, to the results that appear outside” (Chubinsky, 1982). The main characteristic of a motive is awareness. It is necessary to achieve a goal. In this direction, one can agree with B.S. Volkov, who believed that “motive, consciousness, will and other psychological signs appear in unity and interdependence” (Volkov).

The goal is what the criminal is striving for. It is a certain result of the motive for the crime, its model, or, according to A.V. Borzenko, “an ideal image of the desired future result of human actions” (Borzenkov, 1987).

The motive and purpose are optional signs of the the crime subjective side of the crime; there is an inextricable link between them, and they are spelled out in the disposition of the criminal law.
There are various classifications of motives for crime in the legal literature. The researchers P.S. Dagel and D.P. Kotov divided motives into situational (random) and personal (stable) motives. The classification proposed by these authors was the following:

1) “basic”, socially dangerous motives (political, religious, personal “basic” motives);
2) socially neutral motives (resentment, material interest, enthusiasm, etc.);
3) socially positive motives (social interests, altruism, protection of personal rights, friendly feelings, etc.) (Dagel & Kotov, 1974).

Also there is an opinion that the motive can be targeted, orienting and technical, contributing to the selection of both an object and the way of behavior (Sklyarov, 2004). Such a division is also permissible, since the levels of goal setting can be different, determining one or another level of motivation.

T.A. Plaksina believes that the motive and purpose can determine the social danger of a crime, taking into account their inherent dynamic characteristics (Plaksina, 2006).

Motives and goals are diverse (Efremova, 2017; Rogova et al., 2016; Efremova et al., 2019). Often they are characterized by different content, strength, as well as the ability to be updated and by other characteristics.

4 Conclusions

Let's consider the main motives and goals of committing crimes against information security.

1. Selfish motives. First of all, selfish motives in the field of crimes against information security have a financial basis. So, fraudsters focus their activities on confidential information obtaining regarding the data of citizen bank cards, access to the accounts of legal entities with the aim of stealing money. Besides, often the personal data of citizens becomes the prey of criminals. The stolen data used first for criminal purposes: to obtain a loan, draw up false transactions, buy and sell real estate, etc.

In the banking sector, selfish motives can also be performed in the field of transferring funds from one account to another, and during manipulation with the official duties of specialists who have access to the bank information resources.

Another direction for the implementation of selfish motives is the spread of malicious programs to penetrate into information systems of citizens and organizations and obtain some expensive information.

Sometimes they commit crimes in order to get software or databases free of charge, which also become the subject of sale.

2. Hooligan motives. This motive is quite common, usually minors commit crimes in the field of information security from hooligan motives. In particular, they may commit unauthorized access to the databases of large companies, including financial ones, in order to destroy information stored on some server.

3. Revenge. This motive is also often present when they commit crimes against computer security. The subjects of such crimes are the persons who try to avenge, for example, in their opinion, for the unjustified dismissal from work. For this reason, using unauthorized access, such persons penetrate the information systems of the revenge object and destroy or damage the software, which often has nothing to do with the reason for revenge.

4. Commercial espionage, diversion. The motive here is the desire to obtain the necessary information for its subsequent transfer for remuneration to third parties or, conversely, the public dissemination of information that discredits the object of the infringement. Often, criminals, after gaining access to personal data of clients (mobile or insurance company, banking organization, etc.), make them publicly known. Since such data is a trade secret, a number of company customers are often forced to refuse the services of this company after the dissemination of such information because they violated the terms of data confidentiality.

5 Conclusion

Thus, it can be concluded that the motive for crimes against information security is a deliberate motivation. After the motive implementation the subject is able to satisfy his own needs through the commission of a crime. If you establish the motive, you can get the answer to the question why the crime was committed. The goal is the result image, which is important for the subject upon the commission of a crime. If the goal is set, then, accordingly, there is an answer to the question why the crime was conceived and committed.

Acknowledgements

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University.
This paper is a result of scientific research, conducted by six authors, whose contributions are as follows:
Alexandra Yuryevna Bokovnya – writing of the original draft of the paper based in the research results;
Ildar Rustamovich Begishev - references work and data analysis, editing of the final text of paper;
Albina Aleksandrovna Shutova – main idea, conceptualization;
Diana Davletovna Bersei- methodology and results;
Elena Anatolievna Pershina - project supervision, communications;
Valery Pavlovich Potudinsky - proofreading of the final version of the research paper.

Literature:

1. Begishev I.R., Khisamova Z.I., Bokovnya A.Y.: *Information Infrastructure of Safe Computer Attack* // Helix.. Vol. 9, No 5, 2019. Pp5639-5642.
2. Begishev I.R., Khisamova Z.I., Mazitova G.I.: *Criminal Legal Ensuring of Security of Critical Information Infrastructure*

of the Russian Federation // Revista Gênero & Direito.. Vol. 8, No 6, 2019. Pp283-292.

3. Begishev I.R., Khisamova Z.I., Nikitin S.G.: *The Organization of Hacking Community: Criminological and Criminal Law Aspect*s // Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology.. Vol. 14, No 1, 2020. Pp. 96-105.
4. Bokovnya A.Y., Khisamova Z.I., Begishev I.R.: *Study of Russia and the UK legislations in combating digital crimes* // Helix.. Vol. 9, No 5, 2019. Pp5458-5461.
5. Borzenkov A.V. *The goal problem in social development. Abstract from the dis*. by the PhD in Law. M., 1987. 30 p.
6. Chubinsky M.P.: *The motive of criminal activity and its significance in criminal law*. Yaroslavl, 1990, 1982. 180 p.
7. Dagel P.S., Kotov D.P.: *The subjective side of the crime and its determination*. - Voronezh: Publishing house of Voronezh University, 1974. 243 p.
8. Efremova M.A.: *Social Conditionality of Criminal Law Protection of Information Security in the Russian Federation* // Vestnik Permskogo Universiteta. Juridicheskie Nauki = Perm University Herald. Juridical Sciences.. Is. 36. , 2017. Pp222-230.Efremova M.A. The protection of information constituting commercial, tax and banking secrecy by means of criminal law // Vestnik Permskogo universiteta. Juridicheskie nauki = Perm University Herald. Yuridical Sciences. № 1 (27). 2015. Pp. 124-132.
9. Efremova M.A., Rogova E.V. et al.: *Trends of Modern Russian Criminal Policy in the Russian Federation* // Journal of Advanced Research in Law and Economics.. Vol. 10, No 1 (39). , 2019. Pp144-154.
10. Khisamova Z.I., Begishev I.R., Sidorenko E.L.: *Artificial Intelligence and Problems of Ensuring Cyber Security* // International Journal of Cyber Criminology.. Vol. 13, No 2. 2019.Pp, 564-577.
11. Kurushin V.D., Minaev V.A.: *Computer crime and information security*. M.: New Lawyer,1998. 256 p.
12. Malik M.S., Islam U.: *Cybercrime: an emerging threat to the banking sector of Pakistan* // Journal of Financial Crime.. Vol. 26, No. 1, 2019. Pp. 50-60.
13. Martirosyan T.A.: *Legal support of RF information security: abstract from the dis*. by the PhD in Law. M., 2005. 26 p.
14. Mnatsakyan A.V.: *Classification of crimes against the RF information security from the point of view of the current socio-political situation* // Problems of Economics and Legal Practice.. No 2, 2014. pp. 270-273.
15. Plaksina T.A.: *Social grounds qualifying the murder of circumstances and their legal expression in signs of corpus delicti*: Abstract from the dis. by the PhD in Law: 12.00.08 / Plaksina T.A. Tomsk,. 2006. 488 p.
16. Polyakova T.A.: *Legal support of information security in the development of the information society in Russia*: abstract from the dis. by the PhD in Law. / Polyakova T.A. M., 2008. 38 p.
17. Rogova E.V., Karnovich S.A., Ivushkina O.V., Laikova E.A., Efremova M.A.: *State of the Contemporary Criminal Law Policy of Russia* // Journal of Advanced Research in Law and Economics.. Vol. 7, No 1. 2016. Pp. 93-99.
18. Shepetko V.A.: *Features of the legal regulation of crimes against information security* // Scientific aspirations.. No. 20. 2016. pp. 212-214.
19. Sklyarov S.V.: *Guilt and motives of criminal behavior*. - St. Petersburg: Legal Center Press, 2004. 326 p.
20. Volkov B.S. *Motives of crime. Kazan,*. 150 p.

Primary Paper Section: A

Secondary Paper Section: AG, AD