The use of IT technologies in the prevention of crimes

Pavel Ivliev[1*], *Ekaterina* Ananyeva[1], *Irina* Prys[1] and *Yulia* Burbina[1]

[1] Academy of the Federal Penitentiary Service of Russia, 1, Sennaya st., Ryazan, 390000, Russia

Abstract. The importance of information technology in the fight against crime cannot be overestimated in the modern world. It is the use of computer software and appropriate technical means that have become the most effective measures to neutralize and eradicate offenses in practice. Of particular importance are analytical information systems, which can allow through information and communication technologies to solve the main problem, that is, in the disclosure and investigation of crimes. And the most important thing is that the problem of a lack of information is being solved, both about the attacker himself and about the circumstances of the commission of offenses, since all this data is stored in the computer's memory. The comprehensive use of information support in criminal activities, on the one hand, and the use of various technologies for monitoring and managing information flows from the operational services, on the other, in the modern world inevitably moves to a new quality level. Significant advances in the fight against crime can be achieved with the use of modern information technologies and technical means of intelligence purposes. Such a term as "information war" today is filled with a new meaning, expressed in the confrontation between the criminal world and law enforcement agencies. This work is devoted to the study of the issues of large-scale application of information technologies in the field of combating crime in Russia. The problems faced by the Russian society in general and law enforcement agencies in particular are analyzed. Topical issues of the prospects for the effective use of digital technologies in the field of combating crime are considered.

1 Introduction

In the 21st century, it is very difficult to imagine the fight against crimes without the use of modern information technologies. This makes it possible to speed up the process of confronting offenses, reduce the number of law enforcement officers and the burden on the law enforcement system. The relevance of the use of special software and technical devices is provoked primarily by the fact that the fight against organized crime is extrapolated to all spheres of public life, including the information component, which will inevitably increase in percentage compared to other crimes. And in this regard, it is necessary to provide for all sorts of special means and special methods of fighting crimes in the field of information. It

* Corresponding author: a.copytowa@yandex.ru

should be noted that in the context of global informatization of society, the key aspect of social development will be information and communication technologies, which will be aimed at providing the required information to the end consumer, as well as ensuring its safety and processing. Based on this, an increase in the efficiency of law enforcement agencies cannot be achieved without large-scale integration and the introduction of modern information technologies. This is largely due to the fact that a lawyer needs to deal with huge volumes of various kinds of legal information, which in the modern world cannot be dealt without appropriate technical devices and software.

The aim of the study is to analyze topical issues of improving information technology and the use of technical means necessary for an effective fight against crime. To achieve this goal, it is necessary to solve the following tasks:

– to characterize the current state of the digital method of combating crime, used by law enforcement agencies;

– to consider the key problems associated with the use of information technology in modern law enforcement practice;

– to identify promising ways to solve problems associated with the use of digital technologies in the fight against crime.

2 Methods

Aspects of the full-scale application of information technology and special technical devices have been the subject of all kinds of scientific research. So, Vyazovets R.N. worked out the issue of the effectiveness of the use of information technology, systems "Use of information technology in the fight against crime" [1]. G. Gasparyan's research touches upon an actual and effective way of fighting information crimes - citizens' awareness through the state's propaganda activities [2]. Alpeeva O.I. and Bushueva A.V. analyze a very ambitious way to combat information crimes, which is called content marketing [3]. Postnikova K.A. in her research reveals the problem of the use of technical devices, as well as the use of information technology in the activities of law enforcement agencies [4]. Belozerov O.I. and Andreychenko P.M. in their work highlighted the aspects of legality that relate to the introduction of modern technologies in the fight against crime [5]. In addition to the above, modern Russian science contains other studies on this problem, but nevertheless, until now, these issues are not fully worked out and resolved.

In the course of this research, various general scientific and private scientific methods of cognition were consistently applied. For example, at the initial stage of the study, when studying the issues of the formation and application of information technologies in a local historical perspective, as well as abroad, historical and comparative legal methods were used. This made it possible to formulate the unequivocal advantages of using digital technologies and special means in the field of combating crime.

At the second stage of the study, when analyzing the problems of mass introduction and application of digital technologies to combat crime, the method of theoretical analysis and generalization of data was used. This made it possible to identify the most pressing problems associated with the use of digital technologies, which are faced by Russian society in general and law enforcement agencies today.

At the final stage of the research, the dialectical method of cognition was used. The same method, along with the method of formal logic, was used to determine the ways and means of effectively combating crime in the field of information, through the use of various kinds of information resources and special technical means.

3 Results

The conducted research demonstrates the objective inevitability in the use of various kinds of digital technologies and specialized technical means in the fight against crime. Ignoring this fact is extremely negative and will definitely inevitably affect the security of citizens and the entire state as a whole. It is necessary to understand that the transition to the digital age in many ways "unties the hands" of criminals. If earlier, in order to commit a crime, the obligatory face-to-face presence of fraudsters was necessary, which forced criminals to often abandon their atrocities, today, through the Internet, attackers can form an illusion of security, which will provoke them to commit a greater number of crimes. It should be noted that the number of Internet users, as well as people using gadgets, will inevitably grow every year, which in turn will only stimulate the development of information crimes (this fact is reflected in Figure 1). That is why it is very difficult to consider security issues in this area without the full-scale implementation of modern information technologies, security systems, technical devices, and qualified personnel in this area of activity.

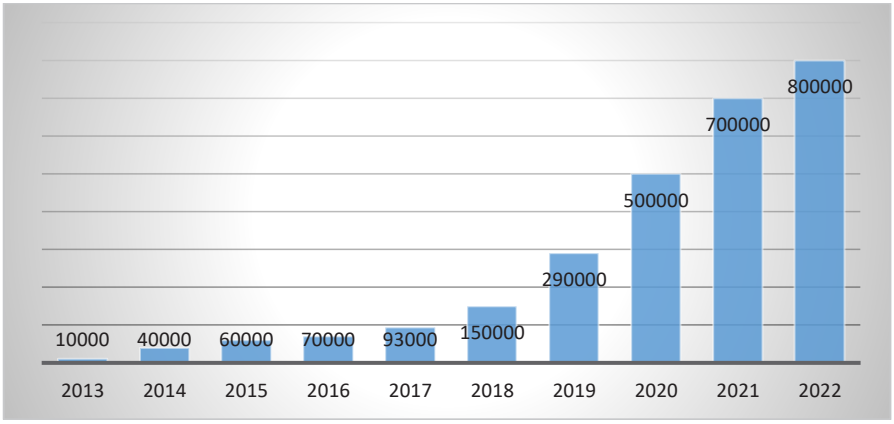

Fig. 1. The number of crimes committed by using information technologies

4 Discussion

The development of information technology and, as a consequence, the emergence of information crime originates in the relatively recent past since the advent of the Internet. The global world wide web began to appear more or less actively in the late 80s of the last century in the United States. But at that time, there were very few citizens with the appropriate equipment to use the network, and because of this crime could not appear in this area. At the same time, the infrastructure was of extremely low quality and, based on this, there was no fertile soil in the world for the emergence of all sorts of information crimes and as a consequence of law enforcement agencies fighting this phenomenon. But the situation began to change already in the 90s of the 20th century in the USA, when already quite a large number of citizens began to have cell phones, all kinds of e-mails and, of course, computers. It should be noted that at that time, various databases began to appear actively in the American state, which contained information about criminals and other statistical data necessary both for combating crime and for anything else. At the moment, fertile soil was formed for the rapid emergence of information crimes. In the late 1990s, the US Congress held hearings on the connections between the Internet and terrorism. Already at that time it was clear that information about the location of chemical weapons, about the

potential death toll and much more could be posted on the World Wide Web. And after the well-known events of September 11, 2001, the US government began to seriously fight Internet crime, which found its expression in the blocking of terrorist accounts. It should be noted that after this terrorist attack, any action that can lead to unauthorized entry into the computer will be regarded as an act of terrorism, and accordingly the provider is obliged to provide all the necessary information about this at the first request of the FBI. It should be noted that certain US states also have criminal legislation aimed at combating computer crimes. For example, the Criminal Code of the state of Texas establishes a provision according to which the acts of a person will be qualified as criminal if the person knowingly uses a computer, network or system without the formal consent of its owner or other authorized person who can give such consent. At the same time, the person committing this act is deliberately aware that there is a protective system of this computer or network, which should prevent data loss. From the content of this provision, it can be concluded that a necessary and sufficient condition for the initiation of criminal prosecution in the commission of a crime in the field of computer information is the mandatory availability of protection of this information [8].

The UK also has extensive experience in fighting information crime. The United Kingdom is one of the world's leaders in damage inflicted by cyber-hackers in the tens of billions of pounds. That is why the UK legislation is quite strict in this area. For example, in 2006, the United Kingdom passed the Police and Justice Act. This legislative act amended the Law on the Misuse of Computer Technologies. In particular, the maximum prison sentence for offenses falling under section 1 of the original version of the Act was increased from six months to two years; the wording “unauthorized modification of computer materials” has been changed to “unauthorized actions that intentionally or through negligence interfere with the normal operation of a computer, etc.”; the maximum sentence under this article was increased to 10 years in prison [6].

It should be noted that Germany has faced the problem regarding crimes committed in the information sphere, too. For example, among the terrorist organization ISIL, banned in Russia, there are citizens of the Federal Republic of Germany in the Middle East. These militants have formed stable groups engaged in recruiting new fighters using the resources of the Internet, and in the prevailing conditions, they use the global network to coordinate the actions of their comrades-in-arms [7]. In general, it should be noted that German legislation is much more lenient in relation to criminals than in the UK. So in the Federal Republic of Germany, preference is given to precisely preventive measures, but as for more radical, that is, repressive measures, they are used extremely rarely, since, in the opinion of the legislator, they can pose a threat to civil rights and freedoms. But unfortunately, such soft measures have not yet been able to help German law enforcement agencies effectively prevent cases of crimes in the field of information technology.

The French Criminal Code contains methods of combating computer crimes that are very unusual for Russian reality. For example, within the framework of the chapter on encroachments on the automated data processing system, not only the possibility of bringing legal entities to criminal responsibility is indicated, but also a detailed list of punishments that can be applied to legal entities for committing these crimes [9]. For example, the French criminal law provides for a fine for encroachments on the automated data processing system on legal entities in five times the fine for similar crimes committed by individuals.

Summarizing the above, we can make a conclusion that the fight against crime in the information sphere takes place in almost all countries of the world, especially in developed countries, but yet no one succeeded in defeating this ailment. It should also be noted that there is an increase in crime in the field of information technology. Many factors contribute

to this. Let us analyze them using the example of Russia, although we can say that many of these factors are also characteristic of foreign countries.

One of the most serious obstacles that the law enforcement system faces in the fight against information crimes is the problem of registration systems, which is quite difficult to optimize their structures. After all, criminals constantly use new ways of committing crimes, thereby forcing the relevant technical specialists in law enforcement agencies to develop new high-quality software in order to effectively combat crime. At the same time, it is necessary not only to keep up with updating the software, but also to be able to combine it with other subsystems and effectively establish interaction between them using computer technologies. And this, in turn, is a rather long and complicated bureaucratic procedure, which, unfortunately, can lead to the fact that criminals will have new possibilities to commit crimes.

Paradoxical as it may sound, but one of the most odious problems associated with the fight against information crimes is the fact that often victims of computer crimes do not always notify law enforcement agencies about the acts committed against them, since they have special reasons for hiding them. These include the undermining of business reputation, and the loss of authority as a specialist, and much more [1].

Another important problem in this area is the fact that software development requires a lot of time and money. After all, as you know, writing software is a complex intellectual task and specialists who are engaged in this require high material support. Based on this, it is rather difficult to imagine that law enforcement agencies are capable of maintaining entire staffs of programmers who will perform their professional activities with high quality. Of course, programmers can be kept out of the state, that is, using such a fashionable tool in our time as outsourcing, but then the problem of operational interaction with law enforcement agencies and the prompt creation of the required software appears. In this situation, the very fact of using the necessary software to combat crime is largely leveled, because what is the point in using information technology in order to effectively combat crime if attackers go one step ahead.

The lack of judicial and investigative practice also negatively affects the disclosure of this type of crime [10].

At the same time, it is necessary to understand that in order to initiate a criminal case, there must be data on the crime committed. The point is that if an ordinary burglary is committed, then the investigator will have at his disposal a fairly wide range of tools that allow him to quickly solve the case. This can be evidence, and sweat traces left by the attacker or other material clues that facilitate the work of the investigator. When committing computer crimes, it is much more difficult to trace the mechanism of the act, because it is unlikely that it will be possible to catch the attacker red-handed, and there will be no witnesses either. At the same time, it is necessary to understand that attackers use fake accounts, change IP addresses with a high frequency, and it becomes almost impossible to track the location of the criminal. This is another and, perhaps, the most important problem in the fight against computer crimes, since many cybercrimes are committed from abroad, then even if it is possible to track the criminal, it will hardly be possible to bring him to justice.

Another rather extravagant problem in the fight against information crimes is the very use of various kinds of technical means, or rather the ethical aspect of this. So, modern history knows precedents when law enforcement agencies used surveillance cameras to catch a criminal. A video surveillance camera recorded the fact of the crime, and in order to detect the criminals, the investigators published this record through the mass media. It seems that there is nothing immoral in this action of the investigating authorities, and moreover, their measures made it possible to calculate and find the criminals, but only in

this video there were a young guy and a girl in the background. The day after the publication, the registry office received two applications for divorce.

It is also necessary to note one more problem associated with the use of special technical means in the field of combating crime. In this situation, we are talking about all the well-known cameras that record traffic violations. Unfortunately, in the modern history of Russia, there are cases when the above cameras were set to a lower speed of movement, and thus this led to the fixation of a violation, which in reality did not exist. Even the President of the Russian Federation spoke out about the inadmissibility of this kind of abuse. At the same time, it is necessary to understand that cameras are also largely installed in places for the purpose of making a profit, and not in order to prevent the commission of violations of traffic rules. This problem also needs to be addressed immediately.

Moving on to the final part of our study, concerning measures to combat information crimes, it is necessary to note their structure (Figure 2), which will make it possible to correctly allocate state resources to combat this problem.

.

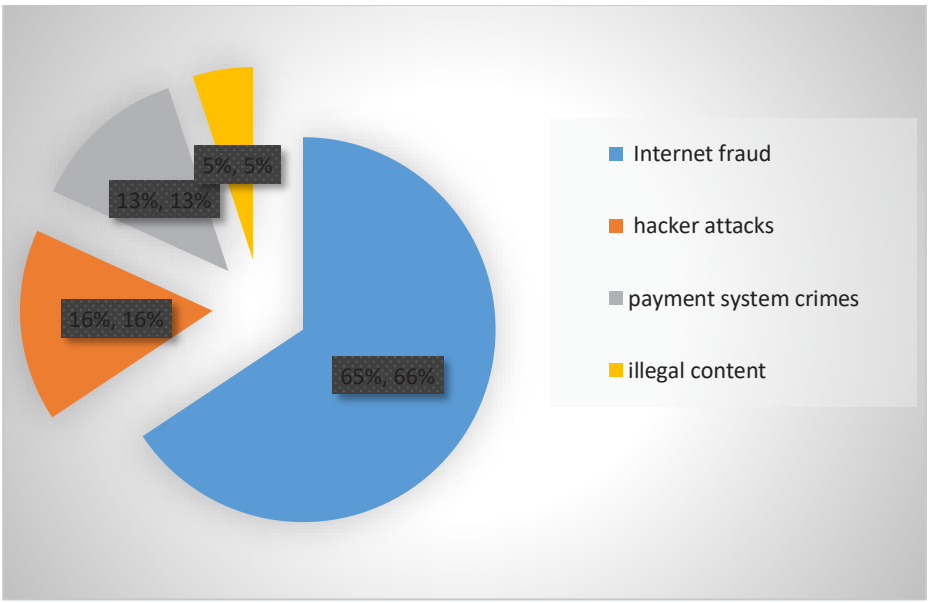

Fig. 2. Types and percentages of information crimes

The fight against information crime is a new phenomenon in modern Russia. Law enforcement agencies, unfortunately, do not have sufficient experience in dealing with this disease. At the same time, we can say with confidence that the number of crimes using digital technologies will only grow, because every year the population will have more and more kinds of technical devices for accessing the Internet, obtaining various services, buying goods and just for fun. Russia, in fact, like the entire civilized world, inevitably stepped into a new era, the age of computers and high technologies, and the transition to an information society is inherently objective for the whole world and cannot be banned or canceled. All this will inevitably create a very fertile ground for the emergence of fraudsters in the information environment. The fight against computer crimes will inevitably cover information spheres, which include the media, as well as telecommunications, global computer networks, as well as various information services industries.

It should be noted that higher educational institutions in Russia currently do not train specialists in the required number in the field of information security. Basically, universities focus on theory in this area and graduates have only general knowledge, which

does not correspond to the modern conjuncture. To eliminate this gap, it is necessary to create a favorable legal environment and highly qualified professionals, as well as create the necessary conditions and technical equipment for educational institutions.

International cooperation is a fundamentally important aspect in resolving cybercrime issues. After all, many criminals who attack our citizens or organizations are located abroad, and even if it is possible to calculate them, it will not be possible to bring them to justice without the appropriate assistance of the state in which the cybercriminal is located. Therefore, the conclusion of relevant international legal agreements on the extradition of criminals or the implementation of one or another assistance between states aimed at combating cybercrime is in many ways a vital process.

Law enforcement agencies of the Russian Federation are faced with the problem of insufficient funding in the fight against computer crimes. It should be understood that criminals have the most advanced equipment and if the state does not properly provide law enforcement agencies with appropriate equipment and technical means, and also does not increase the material content of its employees, then criminals will always be one step ahead.

In order to significantly increase the effectiveness of countering information crimes, it will not be superfluous to use the capabilities of special intelligence equipment. To implement this, it will be necessary to form and develop fundamentally new areas of information and technical support for investigative and operational search activities.

One of the most effective ways to combat information crimes is the creation and implementation into practice of authorized systems, which are studied by a huge number of parameters and characteristics. It allows you to select and classify similar crimes that can be committed by the same offender [1].

Effective crime prevention is possible when society and the state act to achieve the same goals. Fighting computer crimes should not be the sole prerogative of law enforcement agencies. State structures through the mass media should teach citizens an effective response to committing in relation to their offenses in the area we are researching. National governments should launch advertising campaigns to help people protect themselves from such crimes. Simple security measures, especially among young people, can significantly reduce crime rates [2].

Due to the fact that crimes in the information environment have gained momentum in technically developed Western countries, it was not at all logical to use their experience in the fight against this disease. For example, in the United States of America, artificial intelligence has been used in the fight against crime for several years. Analytical software complex CEG (USA, 2016) – using artificial intelligence, the risk of committing a crime in a certain area is analyzed, based on data obtained from social networks, video cameras, weather forecasts, etc. [3]. It also seems advisable to improve methods of crime prevention, not only through artificial intelligence and various kinds of digital technologies, but also through the active use of criminal analysts. This institute has proved itself quite well in a number of European states and the United States. The tasks of criminal analysts are the introduction of new tools to combat criminals, the active use of mathematical analysis, the use of analytical calculations in order to predict crime. It should be understood that these employees must have vast knowledge in the field of software and computer technology.

The creation of a single information space by our state should become one of the priority goals in terms of equipping law enforcement agencies. It must be assumed that in realizing this goal, it is necessary to ensure coordination and close interaction between the authorities. In addition, the creation of a single information space requires the development and integration of existing information and analytical resources, information and telecommunication systems, ensuring the establishment of close interaction not only between the state authorities themselves, but also with the population of the country [4].

At the same time, it is necessary to understand that all law enforcement activities related to the fight against crimes in the information environment, and not only in it, should take place "unnoticed" for the bulk of citizens. This means that people should live their own lives and enjoy all the legitimate benefits of civilization. After all, good governance should, in principle, be invisible to the population. The introduction of information technologies should be carried out with the steady provision of the implementation of the constitutional rights of citizens to access information, protect information about private life and personal data. Great sense is given to the computerization of law enforcement work in compliance with the principle of legality and the use of special technical means of information technology [5].

5 Conclusion

In conclusion, it should be noted that the problem fighting information crimes is very serious, capable of significantly disrupting the usual life for citizens. Of course, in Russia, given that the population is quite poor, it is not difficult to assume that the targets of attacks are mainly citizens of wealthy countries, and Russian society is still facing this problem rarely. But the damage that is caused, for example, to legal entities, in particular to domestic banks, can affect the quality of life of the population. Therefore, the state needs to allocate a large amount of resources, financial, legal, material and technical, as well as others in the fight against information crimes.

Acknowledgments

The authors express their deep gratitude to the leadership of the Academy of the Federal Penitentiary Service of Russia for the help and support provided in the conduct of this study.

References

1. Vyazovets R.N. *The use of information technology in the fight against crime*, Labor and social relations 10, 92-96 (2010)
2. Gasparyan G. *Fighting crime in the field of information technologies through prevention, dissemination of information and awareness raising,* Legal regulation of public relations on the Earth and in outer space: collection of conference proceedings, p. 102-104 (2018)
3. Alpeeva O.I., Bushueva A.V. *The use of digital technologies and artificial intelligence in the prevention of crime*, Bulletin of the Penza State University **3(35),** 54-62 (2021)
4. Postnikova K.A. *Modern information technologies in law enforcement*, Skif. Student science questions **4(56),** 312-315 (2021)
5. Belozerov O.I., Andreychenko P.M. *Trends in the development of information technology in the system of law enforcement*, Scientific journal **2(36),** 7-9 (2019)
6. Karamnov A.Yu., Dvoretsky M.Yu. *UK legislation on crimes in the field of computer information*, Socio-economic phenomena and processes **8(54),** 164-167 (2013)
7. Bolychev N.I. *On foreign experience of legal regulation of countering extremism on the Internet,* Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia **3,** 209-214 (2015)

8. Dvoretsky M.Yu., Karamnov A.Yu. *Crimes in the field of computer information in Russia and foreign countries: problems of qualification, criminal responsibility and punishment*, Bulletin of the Tambov University. Series: Humanities **11(103),** 395-399 (2011)
9. Shved N.A. *Comparative analysis of criminal liability for unauthorized access to computer information in the EU*, Bulletin of the Nizhny Novgorod University named for N.I. Lobachevsky **5,** 222-226 (2016)
10. Noskov O.S., Shevchenko R.A. *Countering cybercrime: problems and solutions*, Legal state: theory and practice **3(41),** 118-121 (2015)
11. Geranin V., Zharko N., Zakharova S., Korneev S. *Environmental factors in the proceedings organization on the compulsory medical measures application*, E3S Web of Conferences **258**, 05016 (2021). DOI: 10.1051/e3sconf/202125805016.
12. Korneev S., Pichugin S., Butenko T., Skorobogatova O., Kokambo Y. *Liability for environmental crimes in the non bis in idem principle context,* E3S Web of Conferences **258**, 05021 (2021). DOI: 10.1051/e3sconf/202125805021.
13. Brovkina A., Rudenko A., Korneev, S., Temirkhanov M., Tarakanov I. *Social adaptation of convicts in the urban planning and greening industry*, E3S Web of Conferences **244**, 12014 (2021). DOI: 10.1051/e3sconf/202124412014.