DOI: https://doi.org/10.17816/RJLS60982

Development of Algorithms to Identify, Disclose, and Investigate High Tech Crimes of an Extremist Nature Committed Via the Internet

© V.V. Bychkov, V.A. Prorvich

Moscow Academy of the Investigative Committee of the Russian Federation

***ABSTRACT*:** This article examines the most important problems arising in the detection, disclosure, and investigation of high tech extremist crimes committed through use of the Internet. The main source of legal errors is found through the identification of mandatory and optional signs of crimes of this type according to their deployed criminal legal characteristics, have been revealed. The specific features of seven groups of algorithms are described, on the basis of which proper information support of all kinds of investigative actions can be created. The specifics of this system of algorithms, within an interactive expert framework, allow investigators to receive necessary information support in real time.

Keywords: extremism; extremist crimes; high tech extremist crimes; criminal characterization; crime qualification; legal errors; information support; algorithm; artificial intelligence; interactive expert system.

To cite this article:
Bychkov VV, Prorvich VA. Development of algorithms to identify, disclose, and investigate high tech crimes of an extremist nature committed via the internet. *Russian journal of legal studies.* 2021;8(1):89–96. DOI: https://doi.org/10.17816/RJLS60982

Received: 15.02.2021 **Accepted:** 03.03.2021 **Published:** 22.03.2021

УДК 343.9.01
DOI: https://doi.org/10.17816/RJLS60982

Особенности формирования алгоритмов выявления, раскрытия и расследования «высокотехнологичных» преступлений экстремистского характера, совершенных с использованием сети Интернет

© В.В. Бычков, В.А. Прорвич

Московская академия Следственного комитета Российской Федерации

Аннотация. В статье рассматриваются важнейшие проблемы, возникающие при выявлении, раскрытии и расследовании «высокотехнологичных» экстремистских преступлений, совершенных с использованием сети Интернет. Выявлены основные источники юридических ошибок, возникающих уже на стадии идентификации обязательных и факультативных признаков преступлений данного вида по их развернутой уголовно-правовой характеристике. Описаны содержательные особенности семи групп алгоритмов, на основе которых может быть создано надлежащее информационное обеспечение всех видов следственных действий. Рассмотрены особенности реализации данной системы алгоритмов в рамках интерактивной экспертной системы, позволяющей следователю в режиме реального времени получить необходимую информационную поддержку.

Ключевые слова: экстремизм; преступления экстремистского характера; высокотехнологичные экстремистские преступления; уголовно-правовая характеристика; квалификация преступлений; юридические ошибки; информационное обеспечение; алгоритм; искусственный интеллект; интерактивная экспертная система.

Как цитировать:
Бычков В.В., Прорвич В.А. Особенности формирования алгоритмов выявления, раскрытия и расследования «высокотехнологичных» преступлений экстремистского характера, совершенных с использованием сети Интернет // Российский журнал правовых исследований. 2021. Т. 8. № 1. С. 89–96. DOI: https://doi.org/10.17816/RJLS60982

Рукопись получена: 15.02.2021 **Рукопись одобрена:** 03.03.2021 **Опубликована:** 22.03.2021

Since the 1990s, an increase in extremist demonstrations has been recorded in the Russian Federation [1, p. 60-71]. More recently, there has been a qualitative change in the nature and methods of such crimes, with a significant increase in extremist crimes committed using information and telecommunications networks, including the Internet [2, p. 43-46]. The detection of these crimes, their disclosure, and their investigation are often difficult for law enforcement officers. The use of modern information technologies, including elements of artificial intelligence, by law enforcement agencies will contribute significantly to solving this problem [3, p. 45-50], although it is important to consider the appearance of new issues.

First of all, it should be emphasized that artificial intelligence is defined in the framework of computer science as a complex computer program designed to solve certain tasks without human participation [4, p. 47-50; 5. p. 34-49]. But law enforcement can never be fully automated. Therefore, there are a number of fundamentally new tasks needed to govern the interaction between law enforcement lawyers and artificial intelligence, or rather such a construction of algorithms for such computer programs, which fully fits into the framework of criminal and criminal procedure law.

An analysis of publications on the features of the use of modern information technologies, including the use of various artificial intelligence types by law enforcement agencies, shows that most often they are talking about the use of ready-to-use, "branded" programs developed by large software firms. At the same time, in many cases, they are also talking about target installations related to the processing of big data contained in specialized databases of law enforcement agencies.

In order to identify, disclose, and investigate "high-tech" extremist crimes, it is necessary to use a wide variety of information technologies. At the same time, the activity of both computer experts, who a few years ago announced the creation of their "forensic science" [6], and large computer companies, claiming not only to create computer criminology, but also to apply it in practice [7], is manifested.

To pay tribute to the efforts of scientists and specialists who develop problems of information and computer security, as well as the active position of experienced computer experts, it is necessary to emphasize the occurrence of the high level of risks in committing various types of legal errors, which can have a negative impact on the entire criminal justice system. First of all, we are talking about the fact that within the framework of information technologies offered to investigators, computer programs created by large Western firms are predominant. Moreover, these programs are extremely complex and are managed by super programmers, not lawyers. Even if there is a lawyer or two involved, they rarely have the same level of understanding or familiarity with the software as the programmers do.

But even when leading computer firms take their legal counsel's opinion into consideration when creating complex computer programs, the frame of reference is Anglo-Saxon law. This is particularly evident in the programs proposed for the introduction of computer robots based on neural network algorithms in Russian electronic legal proceedings and even in electronic justice [8; 9, p. 181-184]. This creates an unacceptably high level of risk for legal errors in criminal proceedings. Such errors are especially dangerous when identifying, uncovering, and investigating extremist crimes committed using the Internet. Ideally, companies could form algorithms with the active participation of law enforcement lawyers that can be used as the basis for information technologies that are necessary for investigators and operational staff to significantly improve the effectiveness of the fight against such crimes.

The results of the conducted studies showed that in many cases, when investigating extremist crimes using the Internet, signs of a second crime are identified, which the legislator referred to as criminal acts with computer information. Moreover, the aforementioned activity of specialists in information security and forensic science is aimed at identifying and combating "computer" crimes. Because of this, the use of appropriate information technologies can lead to the rapid detection of crimes. However, signs of extremist crimes committed using the Internet may be obscure or hidden. Information technologies of a universal nature may not facilitate, but rather complicate the work of investigating crimes of this type.

Therefore, when developing problem-oriented algorithms for creating information technologies aimed at improving the quality of the complex tools used to combat modern extremist crimes, it is necessary to use the entire arsenal of criminal law. Accordingly, it is possible to create several groups of such algorithms.

The first group of algorithms is aimed at creating a solid, scientifically based foundation for the entire set of investigative actions aimed at identifying, solving and investigating crimes of the type in question, including interaction with operational officers, experts and specialists. With its use, it is possible to form a detailed criminal-legal characteristic of a particular crime. At the same time, one must consider that the dispositions of criminal law norms on crimes of an extremist nature are a blank slate, and when disclosing their content features using the provisions of civil and special legislation, there is a risk of going beyond the scope of criminal law. Therefore, it is necessary to include a number of procedures for monitoring this activity of the investigator in the algorithms of this group, procedures that do not differ from those developed for other criminal law norms from a practical standpoint [8].

It should be noted that when disclosing the content features of the dispositions for these crimes, it is necessary to consider the presence of contradictions in some provisions of the current legislation on information and information

DOI: https://doi.org/10.17816/RJLS60982

activities[1], electronic document management[2] and electronic signature[3], as well as on technical regulation in this area. We must also consider that in some cases the problems associated with the fact that the content of the relevant legal norms must be disclosed using the provisions of bylaws and other instructional and methodological documents.

Studies have shown that for these and a number of other reasons, investigators often make legal mistakes when identifying the most important signs of extremist crimes committed using the Internet. Therefore, there is an objective need to carry out targeted research and development in order to form "reference" versions of scientifically based and verified by the most important criteria of criminal law detailed criminal-legal characteristics of crimes of the considered type.

On this basis, problem-oriented databases can be formed, containing information complete lists of mandatory signs of "main" and "additional" variants of the composition of "high-tech" crimes with extremist orientation. They are used to create appropriate algorithms for processing the entire complex of information that is important for the proper detection, disclosure and investigation of crimes of this type.

It is important to pay attention to the fact that it is not only about "filtering" the extensive information that can be related, directly or indirectly, to a specific crime. Using the algorithms of this group and based on the detailed variants of the elements of a crime selected from the databases, it is also possible to form a plan of appropriate investigative actions, both when performing a pre-investigation information check and at the initial, subsequent, and final stages at the investigation of the relevant criminal case. At the same time, other groups of algorithms, which will be discussed below, can be used to properly organize the investigator's interaction with operational staff, forensic experts and specialists.

One of the most important features of the first group is the need to differentiate the features of those crime elements that are associated with high-tech extremism. The analysis shows that legal errors often arise, frequently due to incorrect identification of the composition for a particular crime. Most often, this is due to the fact that extremist crimes using the Internet involve illegal penetration into certain information systems, i.e., hacking security systems, including the use of computer viruses and other high-tech techniques. In these cases, we are talking first of all about the commission of a certain crime in the field of computer information, which is provided for in Chapter 26 of the Criminal Code of the Russian Federation.

As a result, the following situations may occur in practice: First, in addition to an extremist crime, a computer crime can also be committed by the same person or persons with certain forms of complicity. It is clear that we are talking about identifying a set of crimes, for the proper identification of signs, disclosure and investigation of which it is necessary to use appropriate information and methodological support based on a certain group of algorithms, the features of which are discussed below.

Secondly, a "high-tech" extremist crime may be committed, and the composition of one from the computer crimes is absent. Accordingly, we are talking about the formation of a very complex corpus delicti, and to identify all its mandatory and optional features, it is necessary to use special algorithms and information support created on their basis.

Third, we may be talking about the commission of one or more computer crimes, with certain signs of an extremist crime, but they are not enough for the proper formation of the composition of this crime according to its detailed criminal and legal characteristics.

Fourth, a detailed analysis of the elements from the alleged crime can also show the absence of such a crime.

Fifth, it can be revealed that there are signs of several crimes of the type in question, as well as certain "related" crimes that can form an ideal or real set of crimes. In such cases, it is important to pay attention to the relevant provisions of the General Part of the Russian Criminal Code, which disclose the criteria for their identification. At the same time, the group of algorithms for information support of the necessary and sufficient complex of investigative actions is characterized by the greatest complexity both in their development and in practical application.

It is clear that when revealing the features of the detailed criminal-legal characteristics from such complex "high-tech" extremist crimes and identifying the entire set of mandatory and optional features, the investigator faces a number of problems that are not easy to solve even with the involvement of the most experienced experts and specialists. Therefore, it is necessary to emphasize once again the need for comprehensive research by scientists and specialists in the fields of criminal law, computer science, and cybernetics. And the algorithms of problem-oriented processing of legal information created on their basis will allow "contrasting" of the whole set of different options for forming the composition of a specific crime, minimizing the risks of committing legal errors.

To inform the practical work of the investigator at this stage of processing the available information about a particular crime, the first group of algorithms can be used to create an appropriate interactive expert system. At the same time, in order to provide not only a quick analysis of the

[1] Federal Law No. 149-FZ dated 27.07.2006 "On information, information technologies and information protection" // Collection of Legislation of the Russian Federation. 2006 No. 31 (part I). Article 3448

[2] Federal Law No. 122-FZ dated 24.04.2020 "On conducting an experiment on the use of electronic documents related to work" // Collection of Legislation of the Russian Federation. 2020. No. 17. Article 2700

[3] Federal Law No. 63-FZ of 06.04.2011 "On electronic signature" // Collection of Legislation of the Russian Federation. 2011. No. 15. P. 2036.

features from numerous options such as those mentioned above, but also the justification of the most suitable for a particular situation with references to the provisions of specific regulatory legal acts, it is possible to use elements of artificial intelligence.

It should be emphasized here that the corresponding computer programs within the interactive expert system allow for the organization of a dialogue between the investigator and the computer. However, this expert system already plays the role of not so much a reference system, like the widely used Consultant Plus, Garant, etc., but becomes a problem-oriented assistant to the investigator, performing his or her specific tasks related to the identification, disclosure and investigation of specific high-tech extremist crimes.

The second group of algorithms is aimed at providing information support to the most important stage of the investigator's practical work on the proper qualification of a specific high-tech extremist crime. Its structure has a number of features due to the target function associated with establishing the mutual correspondence of the initial information received about the committed act, and then the evidence obtained, to the features of a specific crime that were formalized according to its detailed criminal-legal characteristics. To do this, a system of legal identities is formed in parallel-sequential mode.

The left-hand section of each of the identities in this system is consistently filled in with a description of the object's mandatory and optional features, the objective side, the subject, and the subjective side of this crime. In the right-hand section of each identity at the stage of pre-investigation verification, information about the qualified act is placed, and they are sorted according to the content of the attribute that is located in the left part of each identity. At the criminal-investigation stage, a description of the evidence obtained, which has been properly checked and evaluated, is placed in the right-hand section of these identities.

The second group of algorithms is closely related to the first group, since in the formation of the legal identities' system, it is necessary to use the results of the algorithms' application for forming a detailed criminal-legal characteristic of this crime and the formalization of its mandatory and optional features. In this case, several variants of the results of information processing that were obtained using the algorithms from the first group can be used.

The use of the algorithms from the first and second groups within the framework of the interactive expert system discussed above, allows for the creation of a solid, scientifically based foundation for modern information support of the investigator's work on a specific crime. It is important to emphasize that it is not only about the investigator obtaining extensive and legally verified information about the crime, which s/he can use to properly qualify a certain act. The investigator also gains new opportunities to methodically plan their actions on a scientific basis at various stages of detection, disclosure and investigation of high-tech extremist crimes.

In particular, at the stage of pre-investigation verification of information about a certain act, in which it is assumed that there are signs of a crime from the type in question, the analysis of the content features of the formed legal identities' system in most cases shows the presence of certain information gaps in their right-hand section. To fill in these gaps, the investigator, in accordance with the provisions of Article 144 of the Criminal Procedure Code of the Russian Federation, may involve specialists and forensic experts, as well as perform a number of other procedural actions before making a decision to open a criminal case. At the same time, it cannot replace a full-fledged investigation of a criminal case, so the investigator has to make an informed decision on the opening of a criminal case and its justification in the conditions of information uncertainty.

In this situation, based on the results of the analysis of the formed legal identities system, the investigator can not only state the presence of certain information gaps, but also analyze the possibilities of filling them at the stage of the preliminary investigation. This allows the investigator to significantly reduce the level of risks when making a decision to open a criminal case based on the results of a pre-investigation check with proper information support on the basis of the interactive expert system described above, using the algorithms of the first and second groups.

During the preliminary investigation, the right-hand section of each of the legal identities is formed on the basis of the evidence obtained by the investigator, which must be properly checked and evaluated in accordance with the requirements of Articles 87 and 88 of the Criminal Procedure Code of the Russian Federation. As a rule, after the completion of the initial stage of the investigation of a criminal case, a number of information gaps can also be identified in the system of legal identities in the already-collected body of evidence. After analyzing their content features, new opportunities are created to adjust the initial plan of the investigation, with its focus on obtaining the missing evidence in the subsequent stage of the criminal investigation. At the same time, various investigative actions can be used based on the provisions of forensic tactics, techniques and methods, including the formation of investigative versions and their verification, interaction with operational officers, specialists and forensic experts.

The algorithms of the third, fourth, and fifth groups can be used for proper information support of the investigative and other procedural actions listed above. At the same time, the third group can be aimed at providing information on the most important provisions of forensic science; the fourth is used for information support of interaction with operational staff; and the fifth is for the specialists and forensic experts.

The sixth group of algorithms is aimed at providing proper information support for the verification and evaluation

of each collected evidence in the criminal case under investigation. Their content is due to the need for mandatory compliance with the requirements of Articles 87 and 88 of the Criminal Procedure Code of the Russian Federation. At the same time, special tools are used to bring evidence of various types to a single information format, while at the same time ensuring control over the preservation of their legal status. Additionally, when comparing evidence during the verification, as well as when comparing each of the evidence with the criteria of relevance, admissibility and reliability established by Article 88 of the Criminal Procedure Code of the Russian Federation for their evaluation, an interactive mode can be used that allows the investigator to make appropriate decisions independently.

The seventh group of algorithms is designed for proper information support of the final criminal investigation stage. First of all, we are talking about establishing the sufficiency of the collected evidence body, which is directly indicated in the requirements of Article 88 of the Russian Criminal Procedure Code. However, the content features of this criterion are not disclosed in this article. Therefore, the first part of this group is aimed at forming the final version of the legal identities' system using the algorithms of the second group already discussed above. After that, an analysis of the information completeness for the resulting system is performed at both the quantitative and qualitative levels.

If information gaps are identified and there are doubts that any evidence in the further consideration of the criminal case by the prosecutor and the court can be excluded (which would prevent the criminal nature of the investigated act from being proven), then it is necessary to return to the previous stage of the investigation and take measures to obtain the missing evidence. But when there are no information gaps in the final version of the legal identities system, the investigator can conclude that the act under investigation includes a crime and make an informed decision on the sufficiency of the evidence collected. At the same time, it also helps investigators make an informed decision on the completion of the preliminary investigation and the transition to the preparation and execution of an indictment in this criminal case.

The information support used for this purpose is based on the application of the corresponding part of the algorithms from the seventh group. This part of the algorithms is coupled with other groups of algorithms described above to ensure that the information obtained at various criminal investigation stages can be used in the indictment. We are not, however, talking about "automatic generation" of the indictment text with the help of artificial intelligence.

With the use of the described algorithms' system in the framework of an interactive expert system, the investigator has the opportunity to receive the information support necessary in real time at any moment, starting with the pre-investigation check, including all stages of the preliminary investigation, and ending with the preparation of the indictment. It should be emphasized that if there is a need to form and compare several versions of the investigation plan and/or investigative versions, as well as any other new information that comes to light while performing procedural actions, the investigator can also receive them in real time.

However, it is not only about new opportunities to significantly reduce the complexity and time required to complete most of the investigative actions. It is equally important to pay attention to a number of new opportunities for significantly improving the quality of investigative actions, which is achieved as a result of processing large amounts of information related to the high-tech extremist crime being investigated, including using elements of artificial intelligence. At present, no investigator is able to process such volumes of information during the detection of this crime type and the investigation of relevant criminal cases. Because of this, only a small part of the information about the facts and circumstances related to such crimes is actually used. And the resulting gaps and contradictions in the collected body of evidence often lead to the collapse of the criminal case in court, which results in a considerable waste of resources.

Thus, in order to create a scientific basis for proper information support for all stages of the investigator's work on extremist high-tech crimes committed using information and telecommunications networks (including the Internet) it is necessary to consolidate the efforts of scientists and specialists to develop a system of algorithms discussed in this article. On their basis, interactive expert systems can be created, allowing the investigator to provide all the necessary information on his or her requests in real time.

REFERENCES

1. Bychkov VV. Dynamics of russian terrorism and extremism in the 21st century. *Investigation of crimes: problems and ways to solve them*. 2018;3(21):60–71. (In Russ.).

2. Bychkov VV. Information and telecommunication networks as a means of committing crimes of extremist orientation. *Herald of the Moscow academy of the Investigative committee of the Russian Federation*. 2020;(3):43–46. (In Russ.).

3. Bychkov VV. Artificial intelligence: public policy and vectors of application. *Crime investigation: problems and ways to solve them*. 2020;(4):45–50. (In Russ.).

4. Bychkov VV, Prorvich VA. Artificial intelligence as a means of countering crimes of extremist orientation committed using information and telecommunications networks, including the Internet. *Herald of the Moscow academy of the Investigative*

committee of the Russian Federation. 2020;(4):47–52. (In Russ.).
5. Bychkov VV, Prorvich VA. Artificial intelligence in the fight against crimes committed for extremist reasons, using the Internet. *Modern criminal procedure law — lessons of history and the problems of further reform*. 2020;(1):34–49. (In Russ.)
6. Fedotov NN. Forenzica is a computer forensics. Moscow: Legal World, 2007. 432 p.
7. Volynskij AF, Prorvich VA. Komp'yuternaya kriminalistika v sisteme ugolovno-pravovoj zashchity «tradicionnoj» i cifrovoj ekonomiki. Moscow: Ekonomika, 2020. 476 p. (In Russ.).
8. Volynskij AF, Prorvich VA. Elektronnoe sudoproizvodstvo po prestupleniyam v sfere ekonomiki (nauchno-prakticheskie aspekty). Moscow: Ekonomika, 2019. 364 p. (In Russ.).
9. Eriashvili ND. New level of development of problems of electronic justice on crimes in the economy. *Public service and personnel*. 2020;(1):181–184. (In Russ.)

СПИСОК ЛИТЕРАТУРЫ

1. Бычков В.В. Динамика российского терроризма и экстремизма в XXI веке // Расследование преступлений: проблемы и пути их решения. 2018. № 3(21). С. 60–71.
2. Бычков В.В. Информационно-телекоммуникационные сети как средство совершения преступлений экстремистской направленности // Вестник Московской академии Следственного комитета Российской Федерации. 2020. № 3. С. 43–46.
3. Бычков В.В. Искусственный интеллект: государственная политика и векторы применения // Расследование преступлений: проблемы и пути их решения. 2020. № 4. С. 45–50.
4. Бычков В.В., Прорвич В.А. Искусственный интеллект как средство противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» // Вестник Московской академии Следственного комитета Российской Федерации. 2020. № 4. С. 47–52.
5. Бычков В.В., Прорвич В.А. Искусственный интеллект в борьбе с преступлениями, совершаемыми по экстремистским мотивам, с использованием Интернета // Современное уголовно-процессуальное право — уроки истории и проблемы дальнейшего реформирования. 2020. Т. 1. С. 34–49.
6. Федотов Н.Н. Форензика — компьютерная криминалистика. М.: Юридический Мир, 2007. 432 с.
7. Волынский А.Ф., Прорвич В.А. Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики: монография. М.: Экономика, 2020. 476 с.
8. Волынский А.Ф., Прорвич В.А. Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты): монография. М.: Экономика, 2019. 364 с.
9. Эриашвили Н.Д. Новый уровень разработки проблем электронного судопроизводства по преступлениям в сфере экономики // Государственная служба и кадры. 2020. № 1. С. 181–184.

AUTHOR INFORMATION

***Vasily V. Bychkov,** candidate of law science, associate professor; e-mail: bychkov_vasilij@bk.ru

Vladimir A. Prorvich, doctor of law science, doctor of technical science, professor; e-mail: kse60@mail.ru

ОБ АВТОРАХ

***Василий Васильевич Бычков,** кандидат юридических наук, доцент; e-mail: bychkov_vasilij@bk.ru

Владимир Антонович Прорвич, доктор юридических наук, доктор технических наук, профессор; e-mail: kse60@mail.ru