DOI: https://doi.org/10.17816/RJLS76068

The Role of Legal Algorithmic Language in the Identification, Disclosure, and Investigation of Extremist Crimes Committed Through Use of the Internet

© V.V. Bychkov, V.A. Prorvich

Moscow Academy of the Investigative Committee of the Russian Federation, Moscow, Russia

ABSTRACT: For the proper detection, disclosure, and investigation of extremist crimes committed through use of the Internet, it is necessary to create methods for the study of electronic documents and other information contained in systems of various types. At the same time, an important role can be played by information technologies using elements of artificial intelligence, which provide increased capabilities for investigators' intellectual activities as a result of interaction with them using a legal algorithmic language. Toward this end, it is necessary to create several types of local thesauri and formalize the relationships between the concepts included therein. The features of control over the formation of detailed criminal law characteristics of crimes of the type under consideration, as well as the processing of information in electronic digital form to obtain the necessary evidence, along with their verification and evaluation, are discussed.

Keywords: extremism; extremist crimes; investigation; verification and evaluation of evidence; electronic documents; information technology; interactive expert systems; artificial intelligence; legal algorithmic language; local thesauri.

To cite this article:
Bychkov VV, Prorvich VA. The role of legal algorithmic language in the identification, disclosure, and investigation of extremist crimes committed through use of the Internet. *Russian journal of legal studies*. 2021;8(3):27–40. DOI: https://doi.org/10.17816/RJLS76068

Received: 16.07.2021 **Accepted:** 18.08.2021 **Published:** 20.09.2021

УДК 343.9.01
DOI: https://doi.org/10.17816/RJLS76068

Роль юридического алгоритмического языка в выявлении, раскрытии и расследовании преступлений экстремистского характера, совершенных с использованием сети Интернет

© В.В. Бычков, В.А. Прорвич

Московская академия Следственного комитета Российской Федерации, Москва, Россия

Аннотация. Для надлежащего выявления, раскрытия и расследования преступлений экстремистского характера, совершенных с использованием Интернета, необходимо создание методик исследования электронных документов и иных сведений, содержащихся в информационных системах различного вида. При этом важную роль могут сыграть информационные технологии с использованием элементов искусственного интеллекта, обеспечивающие повышение возможностей интеллектуальной деятельности следователя в результате взаимодействия с ними с помощью юридического алгоритмического языка. Для этого необходимо создание нескольких видов локальных тезаурусов и формализация связей между включенными в них понятиями. Обсуждаются особенности контроля за формированием развернутой уголовно-правовой характеристики преступлений рассматриваемого вида, а также обработки информации в электронно-цифровом виде для получения необходимых доказательств, их проверки и оценки.

Ключевые слова: экстремизм; преступления экстремистского характера; расследование; проверка и оценка доказательств; электронные документы; информационные технологии; интерактивные экспертные системы; искусственный интеллект; юридический алгоритмический язык; локальные тезаурусы.

Как цитировать:
Бычков В.В., Прорвич В.А. Роль юридического алгоритмического языка в выявлении, раскрытии и расследовании преступлений экстремистского характера, совершенных с использованием сети Интернет // Российский журнал правовых исследований. 2021. Т. 8. № 3. С. 27–40. DOI: https://doi.org/10.17816/RJLS76068

Рукопись получена: 16.07.2021 **Рукопись одобрена:** 18.08.2021 **Опубликована:** 20.09.2021

Many factors, including quantitative growth and qualitative changes to extremist crimes committed via the Internet [1, p. 43-46; 2, p. 26-31], their growing latency due to the reluctance of social network owners to comply with the requirements of Russian legislation, the activation of "nonsystemic" opposition on other factors require law enforcement agencies to take urgent steps to improve their effectiveness. At the same time, as numerous studies of this area of crime have shown, difficulties with identifying the signs of the criminal acts in question have arisen with the use of modern information technology. An even broader range of such problems refers to the use of high-tech tools by criminals, in both the preparation and commission of such crimes and for their concealment.

Equally difficult problems arise during the detection and investigation of such crimes. In such case, first of all, it is necessary to note that the documentation with which the investigation has to work is electronic or digital. The application of forensic techniques is required to process digital evidence in the detection of traces of crimes and the subsequent gathering of relevant evidence in a criminal case. In other words, a new law enforcement problem is revealed associated with the use of not only outdated techniques, but also with "traditional" approaches to the creation of digital documents and their use as evidence in criminal matters.

According to the discussion of modern criminology in scientific and practical forums over the past few years, few scientists have tried to focus the attention of their colleagues on the need to understand the specifics of the newly developed social relations. In the conditions of transition to a new, informational society and the struggle against fundamentally new manifestations of high-tech crime, traditional forensic tactics, techniques, and methods are far from being as effective as they were a decade ago. However, most of the criminalists' discussion is limited to terminology discussion.

Already the discussion has expanded to what it would be better to call this new section of criminalistics. In particular, in many reports, speeches, and publications in scientific periodicals, there is a debate about the name for the traces left by criminals in electronic documents of various kinds: are they electronic, virtual, or simply digital? The new science, designed to provide investigators with new, scientifically sound tools for combating high-tech crime, is likely to be called computer forensics, as suggested in various legal acts or digital forensics.

The academic nature of such discussions is not without issue because it affects the scientific foundation of criminology, based on dialectical materialism and the reflection theory. Moreover, in recent years there have been various articles published on this problem. These articles draw attention to the need to change the paradigm from "classical" criminology and instead appeal to modern philosophical currents aimed at forming the foundations of the language of multilevel communication, which ensures better mutual understanding between people [3].

The discussion of such philosophical problems is, however, beyond the scope of this paper. Here we only draw attention to the fact that recently many leading scientists have noted a negative impact on training of investigators and methodological support of the practical activity of "scientific separatism" among representatives of sciences from the criminal-legal block [4, p. 175-185]. Overcoming this difficulty would, however, not only consolidate the scientists' and specialists' efforts in creating forensic and expert techniques, but also make a significant step toward the understanding of modern criminal proceedings problems and potential solutions.

Analysis of the current situation as it relates to pretrial proceedings on extremist crimes committed using the Internet shows that one of the main problems is ensuring mutual understanding of all participants in criminal proceedings [5, p. 16-17] rather than the development and application of modern digital information technology. In this case, we are talking about law enforcement and about law making, including the need for recasting the entire system of domestic legal proceedings in the transition to an information society.

In high-level regulatory documents governing the implementation of electronic justice, the creation of electronic justice using computer robots was also considered based on of neural network algorithms. However, such a simplified, purely technocratic approach creates a high risk of the indirect and unintentional introduction of alien Anglo–Saxon law principles into the Russian judicial system [6].

Similar risks arise from using different software for processing electronic documents and information contained on electronic media as physical evidence. In addition, for the detection, disclosure, and investigation of extremist crimes committed with the use of information and telecommunication networks based on the Internet, through extensive use of electronic documents in various forms, such as graphics and text, in tabular and other forms, and in Russian and various foreign languages computer programs created by major Western firms are often used. These complex programs are developed, written, and debugged by specialists who are programmers, not lawyers.

However, even when the leading computer firms create their computer programs with lawyers in mind, we are still talking about those who think in the paradigms of Anglo–Saxon law. The use of such programs in Russian domestic criminal proceedings creates an unacceptably high level of risks of committing legal errors in the detection, disclosure, and investigation of extremist crimes committed via the Internet.

In our previous publication in this journal, we showed that when developing problem-oriented algorithms for creating information technologies that are aimed at increasing the efficiency of all complex means used for fighting modern extremist crimes committed via the Internet, it is necessary to apply all available criminal-law blocking sciences, including computer science and cybernetics. At the same time, attention is drawn to several groups of such algorithms aimed at creating a scientifically sound basis for the entire set of investigative actions aimed at detection, disclosure, and investigation of such crimes, including interaction with operational staff, experts, and specialists, based on a detailed criminal-law characteristic of a particular crime [7, p. 1-8].

Other groups of algorithms are aimed directly at facilitating the investigator's work with electronic documents, as well as with physical evidence containing electronic information important for establishing the truth in the crimes under consideration. This method raises some technical and legal problems, and overcoming them will also require the consolidated efforts of representatives of all of the criminal and legal sciences, computer science, and several other sciences.

First of all, under Part 3, Article 164.1 of the Criminal Procedure Code of the Russian Federation (Code), an investigator has the right to copy information relevant to a criminal case onto his own medium, certifying it with his own protocol, and then to attach it to the criminal case materials. However, to facilitate the subsequent deciphering of electronic information, the detection of encoded information traces that may be in it, and then preparing necessary evidence on the basis of such items, it is necessary to use special software and appropriate expertise in computer information.

In real investigative practice, one often encounters the situation that when obtaining evidence through experts, the investigator receives a written expert opinion that refers to the certified computer programs used by the opining expert. If the specified computer programs are not available to the forensic expert, the investigator may receive a reasoned refusal to perform the assigned forensic examination.

At the same time, it should be noted that under paragraph 9. 1 of article 204 of the Code, the expert must, in his opinion, describe the content and results of his expert examination and also refer to the expert methodology used. This requirement is directly related to the provisions of Articles 87 and 88 of the Code, which regulates the procedures for verification and evaluation of the evidence, including expert conclusions. At the same time, there is no requirement in the procedural law that the certified computer program is an expert methodology or its equivalent. Further, the certifying organizations do not always perform appropriate research to give an opinion on the effect of using specific computer programs to obtain evidence in criminal proceedings.

It is also necessary to consider the peculiarities of digital rights recently introduced in current legislation, which the legislature has linked to relevant information systems and their controllers. At the same time, these types of rights are referred to as proprietary rights, and the legal status of the information systems, as well as the status of their owners, are not well defined. Moreover, it follows from the content of legal norms that in many cases the rules of the relevant information system established by its owner may play a key role. This controlled access creates risks of legal errors when an investigator or forensic expert uses the necessary information or software products from certain information systems to obtain relevant evidence in a criminal case.

It is quite natural to seek a complex solution to the problems associated with the use of electronic documents in criminal proceedings by the prosecution and evidence obtained based on those documents. In this case, we refer to such use as a legal basis of the current legislation that regulates working with electronic documents, including electronic signatures of various kinds, the information on various media, and software for its processing. All this provides various possibilities for the development and the proper description of algorithms designed for information processing within the framework of criminal proceedings and, above all, for preliminary investigation.

Here, several new problems of technical and legal nature arise associated with the use of certain languages for the appropriate description of the previously mentioned algorithms for problem-oriented processing of electronic documents and other information relevant to establishing the truth in a criminal case. When describing the corresponding algorithms in the language of computer science, it may be difficult for lawyers to understand the necessary features. They may attempt to describe the features in "everyday" language, understandable to all participants of criminal proceedings, and thereby create a high risk of committing both technical and legal errors.

Criteria, based on which language can be chosen to describe all the features of algorithms used for processing electronic documents and other information, are set out in Articles 87 and 88 of the Code. These regulate verification and evaluation of evidence in a criminal case. First, evidence obtained using algorithms for processing electronic documents and other information from various information systems, described accordingly, must be presented in a form that would permit its comparison to other evidence, as well as identification of its source. In addition, the description must provide for the possibility of establishing the relevance, admissibility, and credibility of the evidence obtained during the processing of electronic documents.

In sum, the description of the algorithms should focus on unconditional compliance with the requirements of the Code, including the basis of the analysis of evidence in a criminal case, its proper verification, and an assurance that a proper evaluation is made. In essence, these are aimed at the disclosure of the most important concepts in criminal law and procedure.

At the same time, the concepts of electronic documents, information, digital rights, electronic signatures, and many digital matters used in the description of the relevant algorithms are disclosed by various sections of the civil legislation. In this case, we are also considering legal language, but it is language that differs significantly from its previous version, oriented to criminal law and procedure. These terms lend themselves to the combination of their concepts, creating a single language for criminal proceedings, including the use of hypertext technologies, and providing new opportunities for the formation of the basic systems within dynamic thesauruses [8].

Here it is important to pay attention to the fact that, even when creating a unified legal language and increasing the level of understanding for the criminal proceeding participants, where electronic documentation and other information from various information systems will be used, it is inevitable that certain algorithms must be applied, including those with elements of artificial intelligence. In this case, it is not just a question of combining the relevant conceptual apparatuses of criminal law and procedure and civil law on the basis of computer science. Moreover, establishing a hierarchical system of used concepts with the criminal law and criminal procedural law priorities must be established. This hierarchical system should ensure that the system of created linguistic constructions does not exceed the most important provisions of criminal law.

A further and natural step in creating a unified legal language should be the implementation of the “digital rights” system recently introduced into Russian law. The new law creates fundamental new opportunities for controlling the formation of the rules of those information systems related to the digital rights of certain subjects involved in specific crimes of the type in question. Thus, it will be possible also to introduce into this language rules prescribing the corresponding algorithms of processing the diverse information in information systems that attract the attention of high-tech criminals.

In other words, we are discussing the creation of a unified legal algorithmic language to provide proper informational and technological support for investigative actions relating to electronic documents and other information presented on electronic media. Nevertheless, it is necessary to emphasize the fundamental difference of this approach from other concepts of electronic proceedings previously consider.

First, this undertaking is not just about the application of certain information technologies provided to the investigation on electronic media in the form of other documents or physical evidence, but also a new kind of algorithmic language. When using this language, there is a realization of a multilevel dialog between the investigator and his computer, equipped with the appropriate problem-oriented programs and knowledge bases. The above-described information processing algorithms important for determining the truth in a criminal case are thus realized.

To put it simply, the use of this legal algorithmic language allows the practical implementation of this dialog based on t problem-oriented algorithms of information processing, having been given the legal authority to create correspondingly interactive expert systems. It is possible to use artificial intelligence to provide the possibility of quick analysis of the features of numerous electronic documents selecting the applicable conclusions relating to the revealed offenses with references to the provisions of specific normative legal acts.

It must be emphasized that relevant interactive expert systems such as, in particular, widely used Consultant Plus and Garant, allowing the user to organize a dialog between an investigator and his computer according to their functions, already play a role as reference systems, and the means of communication in the new legal algorithmic language. Essentially, a computer equipped with the corresponding software and knowledge bases becomes a problem-oriented assistant to an investigator, performing specific tasks related to detecting encoded information traces for specific high-tech extremist crimes in the electronic documents and data from various information systems. Such programs then form necessary evidence in the relevant criminal case. At the same time, the investigator receives an opportunity to control every step of the computer processing of documented information and by his electronic signature to give the required legal status to the intermediate and final results of such processing in a particular criminal case.

Using such legal algorithmic language creates new opportunities for the development and practical application of “multilayered,” multilevel hierarchical systems of algorithms oriented toward the support of procedural actions of an investigator at various stages of detection, disclosure, and investigation of extremist crimes committed via the Internet. In fact, we are talking about creating modern forensic and expert techniques, using a new legal algorithmic language, allowing the expert o classify and then carry out group processing of different electronic documents and other information the investigator to detect traces of such crimes. Thus, with the use of these techniques, the investigator has an opportunity to form the necessary evidence for the criminal case under investigation.

In other words, the entire complex of techniques for processing electronic documents and other information in various information systems, created through legal algorithmic language, has created interconnections, both direct and indirect, due to the language properties. Therefore, upon revealing traces of the crimes in question with the help of these forensic techniques, an investigator receives the opportunity to connect the revealed crime traces with those types of evidence that can be obtained via the second part of such techniques.

In turn, the second part of this statute, aimed at obtaining the necessary evidence in a criminal case, including the verification and evaluation of that evidence, allows the investigator to connect the whole edifice of this evidence by applying the third part of the complex of techniques under consideration. This third element is aimed at allowing the investigator to establish informational support of the elements of the crime the sufficiency for the collected evidence. This part of the techniques is inextricably linked with the fourth part of the legal structure. This fourth section is designed for proper disclosure of applications of the relevant criminal-law norms, formation of a detailed legal description of a particular crime, and identification of all mandatory and optional features of facts and circumstances constituting the crime, as well as all elements which must be proved under the requirements of the Article 73 of the Code.

Thus, the development of legal algorithmic language creates various fundamentally new opportunities for multilevel informational support of investigative activity based on interactive expert systems. Moreover, the creation of fundamentally new conditions for dialog of an investigator with a computer increases the possibility of forming a collective intelligence connected to artificial intelligence [9, p. 34-49]. We emphasize that in the work of many scientists there has already been detailed disclosure of the inseparable links between language and thinking in any intellectual activity. Undoubtedly, within such a system of combined “artificial intelligence,” created exclusively for criminal proceedings, there must be a strict adherence to the requirements of criminal procedural legislation in the performance of relevant investigative actions.

Still, artificial intelligence plays the role of a reference and information system set up to search and process necessary for an investigator i in real-time. Since interaction with a set of programs that implements the described algorithms of this “artificial intelligence” is carried out in an interactive mode, the procedural actions are always performed by the investigator. In addition, those intermediate results of information processing that an investigator considers critical for determining the truth in a criminal case can be printed by the investigator and certified with his signature. This procedure, it should be noted, greatly increases the urgent need for a solution to the long-standing problem of granting investigators the right of using electronic signatures to certify these electronic documents that were obtained by him personally and are important for determining the truth in a criminal case.

Before that resolution, it is possible to use the special knowledge and professional competence of specialists in the relevant fields, directly connected to the described system of “artificial intelligence”, and possessing the right of electronic signature for electronic documents created by them. Pursuant to Article 58 of the Code, experts have the right to explain issues falling within their professional competence, and the form of such explanations is not prescribed. Therefore, the investigator can involve an expert in the dialog with artificial intelligence computer programs. This expert can then explain the peculiarities of the information obtained from this reference and information system and, if necessary, certify it with his electronic signature. It is also possible to obtain the corresponding conclusion of this expert in hard copy.

Further, the experts involved in the detection, disclosure, and investigation of extremist crimes committed via the Internet play a special role. Therefore, in addition to the experts well versed in software, it may be necessary to involve others who understand the specifics of the vocabulary used by extremists in textual materials, including those associated with various types of extremist activity. Since the organizers of the relevant crimes may be hiding abroad, it may also be necessary to obtain experts with special knowledge of the slang used by extremists from relevant foreign jurisdictions in various world languages.

In addition, it is often necessary to identify signs of extremist crimes in information of a graphic character. Here, it is possible to use several graphic materials, such as images of certain persons, symbols of a political nature, planning and cartographic materials and schemes marking places of gathering for illegal activities, and so on. Processing such materials often requires specialized knowledge and the involvement of specialists with professional competence in gabitoscopy (identification based on images), geoinformation, and other technologies. Such specialists also use certain professional terminology and often their own professional language and terms of art.

Analysis of the most important features of the above problems of detection, disclosure, and investigation of extremist crimes committed using the Internet, as well as new opportunities for their solution, illustrates the following. First, it is necessary to account for the diversity of the techniques used by criminals, including active use of information technology. In this case, we are talking not only about the perpetrators, but also about their instigators, organizers, and abettors, all of whom have access to a wide range of information technologies.

It is clear that interacting at various stages of preparation for such crimes, the parties must use encoded messages for commitment and concealment, including the use of special disguises. Various programming means are used, allowing different information formats to be used to transmit the relevant information. This process makes it extremely difficult to discover the content of these messages for investigators specialists, and forensic experts involved. Even more difficult are the problems of documenting the necessary evidence based on such coded information. Moreover, criminals are becoming more adept at using the most advanced information technologies to achieve their goals. Unlike law enforcement agencies, the criminal’s ability to use high-tech is not limited by the current legislation.

It is obvious that in the fight against high-tech crime, law enforcement agencies do not have the right to stoop to the same methods used by the criminals and ignore the requirements of criminal procedure law. Therefore, there is an obvious objective need for advanced development of specialized information technologies that meet the requirements of current legislation, including creating a special legal algorithmic language, as noted above, for their most effective use by investigators.

The ideal hierarchical system of algorithms, based on which it is possible to create information support for law enforcement agencies, should include algorithms of several kinds. First, it should be possible to establish the mandatory and optional features of a particular crime according to its detailed criminal-law definition. This would allow the investigator to apply the algorithms to perform the qualification of a crime at various stages of the investigation of a given criminal case. However, for this purpose, it is necessary to use an additional group of algorithms, providing the ability to process electronic documents, as well as other data from different information systems containing crime traces.

As mentioned above, combining these algorithms in the form of interactive expert systems with the application of problem-oriented language providing a possibility of using artificial intelligence elements is of critically important. In the framework of algorithmic languages, the transformation of a certain initial data set must lead to a single result. At the same time, this legal algorithmic language should include language constructions characteristic of algorithmic languages. These allow the removal of the ambiguity of implied conclusions, creating uncertainties in the results, an occurrence aptly reflected in the popular saying that a discussion by two lawyers produces three opinions.

However, it is no less important that this algorithmic language be created for the appropriate operation with the necessary problem-oriented information technology, including using elements of artificial intelligence applied to concepts of criminal law and procedure. Therefore, when working on its basic concepts, as well as those algorithms that allow investigators to create new and inferred knowledge, it is necessary to organize a system of controls to ensure that the algorithms do not go beyond the provisions of criminal law and criminal procedure.

An important role in creating such a legal algorithmic language is played by dynamic thesauri, which offer opportunities for formalizing mutual relations of concepts used within criminal law and procedure requirements. Each such thesaurus includes a strictly limited number of concepts used by lawyers in identifying evidence of the crimes in question in certain acts using the Internet, enabling them to make the decision to initiate a criminal case based on the results of preliminary investigation. Then, the thesaurus assists in collecting, verifying, and evaluating evidence at various stages of investigating the criminal case.

Accordingly, each of the thesauri can be oriented toward a certain group with interrelated concepts reflecting the features of the relevant stages of pretrial proceedings for extremist crimes committed using the Internet. The totality of such “local” thesauri, including the system of direct and reverse links between them, forms a single thesaurus of this legal algorithmic language. The advantages of such structuring of a unified thesaurus, including the possibility of controlling the adequacy of the concepts used in each local thesauri and the links between them, as well as the links between local thesauri by the experts, cannot be overemphasized.

For example, the first of the local thesauri could be oriented to create a system of interconnected concepts reflecting the methods of preparation, committing, and concealing the crimes known to the investigation. In this case, the results of various types of examinations, the specifics of the slang used by criminals, and the specifics of the experts’ professional jargon are also considered. The system of connections between these notions, as well as the experience in the investigation of such crimes and the corresponding criminal cases play an important role.

The second local thesaurus is oriented to the system of concepts used in those normative legal acts of criminal and special legislation, which are necessary for properly disclosing the blanket, reference, and mixed dispositions of the relevant criminal-law norms. At the same time, special attention is paid to controlling the meaningful features of the links for these concepts with the provisions of criminal law and procedure.

The first and second thesauri must be considered as vital “paired” thesaurus, with the help of which the investigator not only identifies signs of the crimes in question, but also carries out their proper qualification at various stages of the criminal case investigation. At the same time, the use of this language with paired thesauri creates fundamentally new opportunities in the dialog with the relevant, interactive expert systems.

We are considering here informational support of decision-making in conditions where insufficient information characterizes a qualifying act at the stage of preliminary investigation. However, this provision is not associated with obtaining additional information “by analogy” with already available techniques. With the help of these interactive expert systems, the investigator has an opportunity to reasonably predict the investigation of a given criminal case and adjust the initial plan of investigative actions to prioritize obtaining missing information about the facts and circumstances to be proven.

The third local thesaurus should be oriented to strict compliance with the requirements of criminal procedure when using appropriate information technologies based on interactive expert systems. Here, the system of interconnections between the concepts used, the content features fully defined by criminal procedure, rather than the system of interconnections between them, becomes of paramount importance. In this case, the primary role is played by those “local” algorithms that have been used by the legislature in the framework of law making. In essence, this process concerns the system of evidentiary law, including the standards of proof and limits, ensuring the proper collection and verification, and evaluation of the collected evidence.

The fourth local thesaurus under consideration focuses on information and technological support of investigative actions with the electronic documents and information from various information systems. Its terminology includes, initially, the concepts used in the existing legislation on information, electronic signature, and digital rights, which regulates the relevant areas of relations of digital rights. Of course, a system of formalized mutual relations of these concepts must also apply here.

Finally, the fifth thesaurus collects those concepts used in to investigate criminal cases of the crimes in question, but not included in the first four local thesauri. In addition, it includes certain not yet established concepts, which can be used episodically, but for these, it is necessary to formalize their connections with other used concepts.

Such construction of the local thesauri system has several advantages from providing possibilities of proper control over the formation of each thesaurus, including formalization of relations between the concepts included in them. At the same time, moreover, the control over the proper formalization of forward and backward connections between the most important concepts from different local thesauri is simplified.

It is important to emphasize that the concepts included in each of the local thesauri according to the closed list are strictly limited. As the current legislation improves and investigators gain experience in detecting, solving, and investigating the crimes in question, when the need arises to supplement the original system of concepts with new ones, the entire system of thesauri is likely to be replaced. This approach avoids both the emergence of uncertainties in processing the initial data, as well as obtaining several alternatives, some of which can mislead the investigation.

Here, we should once again consider the main feature of legal algorithmic language, the formation of a single result from processing the initial data. Therefore, its integral part in the form of a single thesaurus, uniquely defining each of the concepts used in this language and the system of relationships between them, is also designed to ensure the preservation of this advantage of algorithmic languages. A similar approach is used in the construction of knowledge banks used in the framework of the corresponding interactive expert systems, which also provides opportunities for more detailed control over the uniqueness of the definition of those concepts that make up their content.

Using the given language in the problem-oriented interactive expert systems opens some new possibilities in the use of artificial intelligence elements for information support of investigatory activity on the crimes in question. In particular, using the second local thesaurus, an investigator can use hypertext technologies for proper formation of criminal-law norms on crimes of the considered type by applying specially selected by artificial intelligence provisions of civil and special legislation.

The specifics of the corresponding algorithms of hypertext technologies for crimes of an extremist nature are determined by the fact that such crimes have already penetrated into different spheres of social relations. First of all, these are:

- crimes committed for extremist motives, directed against life and health (Clause “k”, Part 2, Article 105, Clause “f”. Part 2. Article 111, Clause “f”, Part 2. Article 112, Clause “b”, Part 2. Article 115, 116, Clause “h.” Part 2, Article 117, Clause 2, Article 119 of the Code),
- the constitutional rights of citizens (articles 136, 148 of the Code), general security (terrorist orientation, committed by extremist motives) (Articles 205-208, 212-214 of the Code),
- the foundations of the constitutional order and security of the state (Articles 280, 280.1, 282-282.3 of the Code),
- public morality (Articles 243, 243.4, 244 of the Code), and
- peace and security of humanity (Article 354.1 of the Code) [5, p. 26-31].

It is no less difficult to formulate detailed criminal-legal characteristics of crimes against the security of computer information and computer technology of all kinds, as well as information and telecommunication networks (Articles 272-274.1 of the Code).

The new sphere of social relations associated with legal relations of citizens in the “information space,” “digital environment,” and “virtual reality,” with the constantly changing content of digital rights to computer information on various sites and social networks, is not only extremely complex in structure, but is also quite contradictory in legal terms. On the one hand, this “information” concept is perceived as something intangible, but this “ephemeral reality” is also protected by legislation on state secrets, copyright, property, human privacy, the secrecy of investigations, and court proceedings, and official, professional, and commercial secrets.

In addition, when revealing the content features used in forming the detailed criminal-legal characteristics of the crimes in question, we cannot ignore the established professional jargon of computer scientists, hackers,[1] and experts in various aspects of computer networking and information technology use. Many of these concepts are disclosed within the first local thesaurus. However, to disclose the blanket dispositions of the relevant criminal-law norms and form a detailed description of the various aspects of the crimes in question, the terminology legitimized in the relevant normative legal acts included in the second local thesaurus must be used. To put it differently, all these concepts and the links between them must be properly described within a single language, using the first and second local thesauri, as well as others, in which all the terms used from criminal, civil, and special legislation, and from law enforcement practice, so that the crimes in

[1] A hacker or a “computer hacker,” is a programmer who deliberately bypasses computer security systems.

question will have the same meaning in terms of the current legislation and will not require additional interpretation.

For this purpose, it is necessary to use such elements of artificial intelligence as hypertext technologies and knowledge of engineering and neural network algorithms [8]. With their use, it is possible to form unambiguous and easily understood detailed criminal-law elements of the crimes in question. For this purpose, special research should be completed to ensure that any given deployed criminal-law element does not contradict the most important criminal-law principles and does not go beyond its limits. To achieve this goal, the third and fourth local thesauri can be used within the framework of an appropriate interactive expert system.

Clearly, such special research using the previously mentioned interactive expert systems and legal algorithmic language should initially be performed by experienced specialists who participate in relevant research and development. This limitation will reveal the major problems associated with the practical application of these expert systems to artificial intelligence elements and help to work out the most important features of the legal algorithmic language at the level of its mass application in the system of investigative agencies.

Special research, aimed at organizing the practical use of interactive expert systems, creates an opportunity to work out the primary aspects of consolidating the collaborative joint thinking of scientists and specialists with different artificial intelligence creators. More precisely, we are talking not so much about a new type of thought among a group of law enforcers, including scientists representing various branches of criminal-legal science and specialists-practitioners using a new type of algorithmic language, as we are about the practical application of algorithms to organizing the dialog of these experts with different types of artificial intelligence.

To clarify, we are contemplating the fact that the investigator or expert, who has the necessary professional competence to apply certain types of artificial intelligence with appropriate knowledge bases, will through their new capabilities in processing information relevant to a criminal case be considered more educated or more experienced in practical terms. At the same time, it is important to emphasize that information technologies of artificial intelligence used with the help of legal algorithmic language are applied not so that the investigator can receive from his computer a fast and easy decision. On the contrary, the investigator has an opportunity to quickly receive numerous explanations on virtually any questions that arise, as well as predictions of the consequences that may have been identified during investigative actions. However, after receiving any explanations from the interacting artificial intelligence, the investigator makes the decision solely on his own, guided by his inner conviction based on the law and his experience, as well as knowledge of all the available evidence in the criminal case under investigation.

Here we can draw a certain analogy with the application of the previously described information technology to the investigation of a criminal case by an investigative team formed of investigators who have not only great practical experience, but also professional competence at the level of the professors. After receiving information from each of the group members, the head makes an independent decision not based “averaging” or some other way of combining the proposals of his colleagues, but based on his own inner conviction, formed according to the current legislation requirements.

However, in contrast to the very expensive actions of a large investigative team of the most experienced and knowledgeable staff, the use of interactive expert systems under consideration allows achieving the same result much faster and easier. This is achieved not only by replacing experienced specialists with computer systems, which “keep in their minds” a thousand times the volume of information and process it a million times faster. No less, if not more important, is the fact that the dialog with the head of so peculiarly formed “investigation team” is not in the “normal” Russian language, but in the problem-oriented legal algorithmic language.

Consequently, while processing of the available initial data rather than receiving multivalued variants of possible events’ development, through dialog with the artificial intelligence in legal algorithmic language; an investigator receives a single variant result processing the initial information under the conditions formed by that investigator. Thus, through the analysis of this result, the investigator may consider it necessary to make changes in some of conditions generated earlier. If so, after that dialog with an artificial intelligence, the investigator will receive a unique new result from reprocessing the initial data system. Then, having supplemented or changed the original system of initial data at this new stage of the dialog, an investigator can acquire another unambiguously formulated variant of processing within the formulated conditions, reflecting the features of the criminal case under investigation.

Thus, in a dialog with artificial intelligence in a legal algorithmic language in a short time, an investigator can ask not just a few hundred questions of a reference nature and instantly get the appropriate answers. He also has fundamentally new opportunities to set tasks of varying complexity, for which the solutions are important for proper investigation and immediately receive the necessary results. This new ability significantly invigorates the investigator’s own thinking process and reduces the time needed to consider the possible courses of action needed to make the right decision.

Moreover, since during the investigation of criminal cases, one has to face the necessity of processing different electronic documents, as well as information from different information systems by means of special computer programs, not all members of the investigation team can be useful for this kind of investigation. At the same time, with the help of certain elements of artificial intelligence in the expert system, many fundamentally new opportunities are created for the investigation of features and proper evidence calibration in a criminal case.

It is evident that a significant increase in the effectiveness of investigative actions on extremist crimes committed via the Internet, as well as reducing the time for investigation of such criminal cases, can be achieved by complementing the collective intelligence of an investigator and interactive expert system with the intelligence of additional specialists and forensic experts. At the same time, similar systems can be created to foster a dialog between experts and specialists with artificial intelligence within the framework of such expert systems and knowledge bases.

Several possibilities open up the use of respective information technologies for the performance of investigative actions on examination and evaluation of each collected item of evidence, as well as the determination regarding the sufficiency of the entire set of all collected evidence at different stages of a criminal case investigation. For this purpose, it is possible to use the third local thesaurus for the evidence obtained by studying electronic documents and information from various information systems, along with a parallel use of the fourth local thesaurus.

In order to organize appropriate research and development, to provide the creation of new information technologies that combine the capabilities of the investigator's intellectual activity and certain elements of artificial intelligence using legal algorithmic language, it is important to consider several provisions of recently adopted normative legal acts.

Of importance here is the decree by the President of the Russian Federation dated October 10, 2019 No. 490 "On the development of artificial intelligence in the Russian Federation"[2] The National Strategy for Artificial Intelligence Development for the period until 2030 was approved, with the stipulation that the economy and the social sphere must be defined as the priority areas for the development and use of artificial intelligence technologies. It should be noted; however, that one of the goals of artificial intelligence development, along with ensuring the growth of welfare and quality of the people's lives and ensuring national security and sustainable competitiveness of the Russian economy, also includes ensuring law and order.

The Russian Government's Order No. 2129-r dated August 19, 2020, approved the Concept for the Development of Relationship Regulation in the Field of Artificial Intelligence and Robotics Technologies up to 2024[3] notes that the priority goal of regulating relations in the field of artificial intelligence is to stimulate the creation of artificial intelligence, which will contribute to achieving high rates of economic growth, improving the welfare and quality of the people's lives, while ensuring national security and the rule of law.

Thus, the creation of scientific foundations for a new legal algorithmic language can play a key role in significantly enhancing the intellectual capabilities of the investigator, if its dialog with the artificial intelligence within the framework of appropriate interactive expert systems is properly organized. This organization is of particular importance when investigating criminal cases of extremist crimes committed via the information and telecommunication networks, including the Internet, where there is a need to study numerous electronic documents and information from different information systems.

To implement the relevant part of research and development provided for in the state programs for the development of artificial intelligence mentioned above and ensuring its practical application to strengthen the rule of law in the transition to an information society, it is necessary first of all to consolidate the efforts of scientists and experts in the relevant fields. In turn, it is equally important to locate specific forms of such consolidation for the representatives of the criminal and legal science, computer science, and cybernetics at the interdepartmental and state level. In order to focus the scientists' and specialists' efforts on creating new applicable information technologies for combating modern cybercrime of extremist nature, it is necessary to consider possibilities for the interaction of scientists and specialists working in law enforcement bodies with the representatives of scientific teams from the Russian Academy of Sciences, as well as other leading higher educational institutions of the country.

[2] Collection of Laws of the Russian Federation. 2019. No. 41. Article 5700.

[3] Official Internet-portal of legal information. URL: http://publication.pravo.gov.ru/Document (accessed on: July 15, 2021).

REFERENCES

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

2. Bychkov VV, Rotov VA. The concept and types of crimes of extremist orientation committed using information and telecommunication networks. *Investigation of crimes: problems and ways to solve them*. 2020;(3):26–31. (In Russ.).

3. Sokol VY. Crisis of domestic criminalistics. Krasnodar, 2017. 332 p. (In Russ.).

4. Volynsky AF. Subject of criminalistics and «scientific separatism»: consequences and possibilities of overcoming them. *Proceedings of the academy of management of the Ministry of internal affairs of Russia*. 2018;1(45):175–185. (In Russ.).

5. Bychkov VV, Prorvich VA. Artificial intelligence in the fight against extremism. *Russian journal of legal research*. 2020;7(4): 9–18. (In Russ.).

6. Volynskij AF, Prorvich VA. Elektronnoe sudoproizvodstvo po prestupleniyam v sfere ekonomiki (nauchno-prakticheskie aspekty). Moscow: Ekonomika, 2019. 364 p. (In Russ.).

7. Bychkov VV, Prorvich VA. Features of the formation of algorithms for identifying, disclosing and investigating «high-tech» crimes of an extremist nature committed using the Internet. *Russian journal of legal research*. 2021;7(1):1–8. (In Russ.).

8. Bychkov VV, Prorvich VA. Artificial intelligence in the fight against crimes committed for extremist motives using the internet. *Modern criminal procedure law – lessons of history and problems of further reform.* 2020;1(2):34–49. (In Russ.).

9. Volynskij AF, Prorvich VA. Komp'yuternaya kriminalistika v sisteme ugolovno-pravovoj zashchity «tradicionnoj» i cifrovoj ekonomiki. Moscow: Ekonomika, 2020. 476 p (In Russ.).

СПИСОК ЛИТЕРАТУРЫ

1. Бычков В.В. Информационно-телекоммуникационные сети как средство совершения преступлений экстремистской направленности // Вестник Московской академии Следственного комитета Российской Федерации. 2020. № 3. С. 43–46.

2. Бычков В.В., Ротов В.А. Понятие и виды преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных сетей // Расследование преступлений: проблемы и пути их решения. 2020. № 3. С. 26–31.

3. Сокол В.Ю. Кризис отечественной криминалистики. Краснодар, 2017. 332 с.

4. Волынский А.Ф. Предмет криминалистики и «Научный сепаратизм»: последствия и возможности их преодоления // Труды Академии управления МВД России. 2018. № 1(45). С. 175–185.

5. Бычков В.В., Прорвич В.А. Искусственный интеллект в борьбе с экстремизмом // Российский журнал правовых исследований. 2020. Т. 7. № 4. С. 9–18.

6. Волынский А.Ф., Прорвич В.А. Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты): монография. М.: Экономика, 2019. 364 с.

7. 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. 7. № 1. С. 1–8.

8. Волынский А.Ф., Прорвич В.А. Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики: монография. М.: Экономика, 2020. 476 с.

9. 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. 2000. Т. 1(2). С. 34–49.

AUTHOR INFORMATION

Vasily V. Bychkov, candidate of legal sciences, 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