DOI: https://doi.org/10.17816/RJLS568994

Scientific Article

Computer Modeling of Criminal Manifestations in the Field of Digital Rights: Basic Approaches and Algorithms

V.A. Prorvich

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

Abstract

Considering the substantive features of the digital rights recently introduced in the current legislation indicates that the rules of information systems established by their owners are the most vulnerable to crime. An increased level of risk is created by the possibility introduced by Russian entities to use the digital rights of foreign information systems because their rules do not meet the requirements of Russian legislation. This significantly complicates the disclosure of blanket dispositions of the relevant criminal law norms, which represents the solution of inverse challenges that have a certain analogy with the solution of integral equations with several uncertainties. The described system of computer modeling of criminal manifestations in the field of digital rights covers all challenges, the solution of which will create a modern system of criminal law protection of subjects concerning digital rights. The first part is aimed at preparing and justifying changes and additions to criminal legislation and procedures. The second part covers the challenges of proper information and methodological support for investigative actions concerning the establishment of the subject of proof, collection, verification, and evaluation of evidence in relevant criminal cases. This passage describes the features of the approaches and methods used for the formation of appropriate hierarchical systems of legal algorithms. It also details how the creation is based on the packages of applied computer programs for practical application in an interactive mode.

Keywords: digital rights; rules of information systems; criminal law protection; computer modeling algorithms; computer criminology; subject of proof; limits of proof; computer forensics; interactive expert systems.

To cite this article

Prorvich VA. Computer modeling of criminal manifestations in the field of digital rights: basic approaches and algorithms. *Russian journal of legal studies.* 2023;10(3):7–19. DOI: https://doi.org/10.17816/RJLS568994

Received: 09.08.2023 **Accepted:** 17.09.2023 **Published:** 30.09.2023

УДК 343.9

DOI: https://doi.org/10.17816/RJLS568994

Научная статья

Компьютерное моделирование преступных проявлений в сфере цифровых прав: основные подходы и алгоритмы

В.А. Прорвич

Московская академия Следственного комитета РФ, Москва, Россия

Аннотация

Рассмотрение содержательных особенностей недавно введенных в действующее законодательство цифровых прав показало, что наиболее уязвимыми для криминала являются правила информационных систем, устанавливаемых их обладателями. Еще более высокий уровень рисков создает введенная законодательно возможность использования российскими субъектами цифровых прав иностранных информационных систем, поскольку их правила не соответствуют требованиям российского законодательства. Это существенно усложняет раскрытие бланкетных диспозиций соответствующих уголовно-правовых норм, которое фактически представляет собой решение обратных задач, имеющих определенную аналогию с решением интегральных уравнений с рядом неопределенностей в их левой и правой части. Описанная система компьютерного моделирования преступных проявлений в сфере цифровых прав охватывает весь комплекс проблем, решение которых позволит создать современную систему уголовно-правовой защиты субъектов цифровых прав. Ее первая часть нацелена на подготовку и обоснование тех изменений и дополнений, которые необходимо внести в уголовное и уголовно-процессуальное законодательство. Вторая часть охватывает проблемы надлежащего информационно-методического обеспечения следственных действий, связанных с установлением предмета доказывания, сбором, проверкой и оценкой доказательств по соответствующим уголовным делам. Описаны особенности подходов и методов формирования соответствующих иерархических систем юридических алгоритмов, а также создания на их основе пакетов прикладных компьютерных программ для практического применения в интерактивном режиме.

Ключевые слова: цифровые права; правила информационных систем; уголовно-правовая защита; алгоритмы компьютерного моделирования; компьютерная криминология; предмет доказывания; пределы доказывания; компьютерная криминалистика; интерактивные экспертные системы.

Как цитировать

Прорвич В.А. Компьютерное моделирование преступных проявлений в сфере цифровых прав: основные подходы и алгоритмы // Российский журнал правовых исследований. 2023. Т. 10. № 3. С. 7–19. DOI: https://doi.org/10.17816/RJLS568994

Рукопись получена: 09.08.2023 **Рукопись одобрена:** 17.09.2023 **Опубликована:** 30.09.2023

Since the introduction of digital rights, which the legislature has classified as property rights, into the current legislation under Federal Law of March 18, 2019 No. 34-FZ, new problems have arisen concerning the criminal legal protection of individuals who hold these rights, a group that comprises the majority of Russian citizens. The significance of these problems continues to grow, yet the relevant criminal law and criminal-procedural norms have not been adopted, setting off a chain reaction of problems in law enforcement, particularly in cases involving these rights [1].

The most urgent problem faced in law enforcement stems from the fact that, following the updated wording of Articles 128 and 141.1 of the Civil Code of the Russian Federation (CC RF), digital rights are defined as "obligatory and other rights, which content and conditions for the implementation are determined in accordance with the rules of the information system". However, when introducing the new legal concept of "information system rules", the legislator failed to specify the procedures for their adoption or even the requirement that such rules must comply with the existing legislation. Furthermore, the problem of accountability for their violation remains unaddressed.

Attempts to interpret these legal norms "by default", assuming that all owners of information systems are law-abiding Russian citizens, were invalidated by the legislature. When incorporating provisions on digital financial assets into the current legislation through Federal Law No. 259-FZ of July 31, 2020, it was specified that digital financial assets are defined as digital rights whose issuance, accounting, and circulation are only possible through entries in an information system based on distributed registry. These assets can serve as subjects to mortgages, objects of purchase and sale transactions, exchanges of other types of digital financial assets (including those issued according to foreign information system rules), or digital rights of other types. It is evident that the rules of foreign information systems are not created by law-abiding Russian citizens and do not automatically comply with the requirements of current Russian legislation.

Leaving aside the issues of protecting the digital rights of Russian citizens in foreign jurisdictions, which fall beyond the scope of this article, it is vital to focus on the most immediate problems of a criminal law nature. The absence of criminal law provisions that reveal the characteristics of various types of crimes in the field of digital rights has given rise to new problems associated with the proper interpretation of the broad provisions of existing criminal law norms. This is where the lack of legislative regulation regarding the rules of information systems, which govern the interaction between system owners and their clients, is manifested most clearly This absence gives rise to a host of uncertainties in the classification of such crimes, negatively impacting their detection, resolution, and investigation [1, 2].

Research reveals that the procedures for identifying blanket, reference, and mixed dispositions in criminal law norms, followed by the development of detailed characteristics of specific types of economic crimes, are highly labor intensive [3]. This complexity arises primarily because investigators must consider not only numerous provisions from dozens of federal laws but also hundreds of regulations at various levels. Additionally, the legislator has introduced rules governing information systems, within which a wide array of digital rights transactions occur. Consequently, there is a high level of risk of legal errors due to objective and subjective factors, with the investigator held responsible [4].

Among the objective reasons for these legal errors, we must highlight inherent shortcomings in the approaches used to uncover the blanket dispositions of criminal law norms for crimes, as identified by many legal experts and scholars. According to certain established methods, the investigative process is based on the application of the General Part of the Criminal Code of the Russian Federation (CC RF), followed by relevant federal laws and regulations [5]. In this case, monitoring plays a significant role, ensuring that investigators remain within the scope of criminal law when constructing a comprehensive legal description of the crime under investigation.

From a legal perspective, this approach is completely justified, despite several practical challenges of implementation that heighten the risk of legal errors. However, from a mathematical standpoint, it places investigators in the position of solving an "inverse problem." This is because when developing a criminal law norm, the legislator must consider not only the characteristics of the social relations violated criminals but also elements of civil and special legislation regulating legal relations in the relevant segments of social relations involving economic entities, including business customs.

Furthermore, when forming certain criminal legal norms concerning digital rights, legislators have started using complex mathematical probabilistic models. The identification of the elements of the crime's object and subject, as well as its objective aspects, becomes fraught with complexities when disclosing the blanket dispositions of these norms. This, along with several other objective and subjective factors, contributes to an exceptionally high

latency level in such crimes. This latency primarily applies to a broad spectrum of criminal manifestations related to market manipulation within the digital rights domain [1, 2].

The attributes of the crime's object, as revealed by criminologists within the field of digital rights, require not only sociological research but also the exploration of entirely new aspects of legal relations within the context of transitioning to a new information society. Criminological research that delves into the objective aspects of such crimes, and their subjective aspects is gaining increased relevance. However, this research is time-consuming and remains far from complete, with the application of mathematical modeling to analyze criminal manifestations within the digital rights field still underutilized by criminologists.

From a mathematical perspective, the legislative process shares certain similarities with the convolution of functions involving multiple variables or the formation of integral transformation [6]. Through this "legal convolution" of various provisions within the current legislation, we arrive at a concise expression of the blanket, reference, or mixed disposition of the corresponding criminal law norm. Attempting to reveal such a disposition and establish a comprehensive criminal legal description for a specific crime within the sphere of digital rights represents an "inverse legal problem."

A more detailed examination of the intricacies of this "legal convolution" that characterizes criminal manifestations within the digital rights framework, including the aforementioned problems in forming information systems rules, further complicates the process. At this point, we can draw analogies with the formation of integral equations of various types [7]. Due to uncertainties on both sides of the "legal integral equation", it possesses an infinite number of solutions, thus carrying a high level of risk of legal errors when adapting existing criminal law norms to the digital rights system.

Mathematicians offer various methods for solving such inverse problems, including successive approximation methods based on the theorem of Fredholm et al. For inverse problems plagued by uncertainties, regularization methods have been developed to provide "interval estimates", indicating the possible range of the desired solution. The application of a priori information plays a significant role, paralleling the investigator's task in forming detailed criminal legal characteristics of a crime under investigation while considering all available information.

As the use of various cryptocurrencies in the modern economy expands, diverse scenarios emerge for regulating legal relations among subjects at various levels [8]. Simultaneously, it is necessary to consider the influence of criminal manifestations on each of these scenarios and the measures adopted to mitigate their adverse effect. However, identifying and recording crimes in the field of digital rights, facilitated by blockchain technology, remains a formidable challenge. However, when investigating collections of such crimes occurring before and after the adoption of cryptocurrency, the process of identifying and recording encoded information traces is greatly simplified. In many cases, this involves interval assessments of relevant information regarding the actions of digital rights subjects.

As computer technology advances, direct numerical modeling methods have become increasingly valuable for addressing such problems. By changing the initial data on the left part of the equation within predetermined limits, numerous solutions to the direct problem can be obtained through numerical modeling. These solutions are then compared with the right part of the equation to determine the best match, the desired solution. In some cases, more complex algorithms were used, such as selecting multiple solution options that were further scrutinized with a priori information to obtain the desired solution.

When we apply an analogy to "legal modeling," a concept used by investigators when forming detailed criminal legal characteristics for specific crimes under consideration, we need to focus on several key aspects. These features come into play when defining these problems and developing a system of algorithms for solving them. However, the process of legal modeling of criminal manifestations remains insufficiently formalized, leading to frequent legal errors that adversely affect the entire process of investigating criminal cases.

The research highlights specific aspects related to the formalization of the main stages of such modeling. First, critical provisions used by the legislator when defining the concept of a "crime" in Article 14 of the CC RF, as well as the detailed characteristics of all its elements in the General Part of the CC RF, should serve as basic input data. Additionally, a system of mandatory and optional elements for the most common crimes in the field of digital rights can be treated as "information standards".

To ensure that the criminal legal characteristics of these types of crimes are amenable to computer modeling and support the proper investigation of relevant cases, a set of attributes defining the concept of "evidence" should be incorporated as the second fundamental concept when forming a system of initial data for computer modeling of criminal manifestations in the digital rights domain. This results in two sets of computer modeling tasks, aimed at

DOI: https://doi.org/10.17816/RJLS568994

defining the most important elements of a crime to facilitate proper classification and investigating cases involving crimes in the digital rights domain.

When framing both sets for computer modeling of possible criminal manifestations in the digital rights system, several alternative approaches with varying content can be identified. These approaches can be categorized as "empirical", "theoretical", and "combined".

Empirical approaches are based on existing practical experience in identifying, solving, and investigating these types of crimes. For digital rights crimes, convictions are relatively limited, with the highest number of relevant criminal cases typically associated with fraud using electronic payment methods (Article 1593 of the CC RF), and the lowest number associated with market manipulation (Article 1853 of the CC RF) [1, 2].

During the formalization of the entire body of information derived from these criminal cases, the characteristics related to the object, objective aspects, subject, and subjective elements of various types of digital rights crimes can be identified and organized systematically. This facilitates the comparison of these characteristics with content-relevant criminal law norms and enables the establishment of approaches to uncover blanket, reference, and mixed dispositions used by courts. By examining the results, we can develop recommendations for selecting the most appropriate options for computer modeling of these types of crimes in law enforcement practice.

These recommendations serve primarily to enhance the developed models and algorithms for computer modeling of various types of crimes in the digital rights domain. However, they can also provide a foundation for methodological recommendations for investigating relevant criminal cases involving digital rights crimes, including the development of relevant forensic techniques.

The theoretical approach involves the formation of formalized characteristics of the "legal field". These characteristics reveal the dynamics of interactions between law-abiding digital rights subjects, involving information systems owners and consumers of their services. To achieve this, simulations of such interactions can be based on the totality of provisions with the current civil and specialized legislation, established business customs, and a certain set of "information standards" can be established for the activities of law-abiding subjects in the existing legal framework.

However, the research conducted reveals that uncertainties emerge due to certain inconsistencies in various types of legislation, particularly at the level of by-laws. Furthermore, these inconsistencies are compounded by noted disparities between the rules established by various information system owners and the provisions of the current legislation. These inconsistencies can be addressed through various methods, including the use of empirical data.

When examining theoretical models for deviations from "standard" activities of law-abiding digital rights subjects and identifying the attributes of typical violations of current legislation, it is crucial to consider key criminal law provisions. Not every violation of current legislation by digital rights subjects comprises all elements of a crime, particularly concerning issues related to the subjective aspect of the crime, such as intent, the nature of motives, and the form of guilt.

Modeling these elements of a crime is characterized by significant uncertainties. To address these uncertainties, certain approaches from the field of criminology, along with elements of artificial intelligence (AI) based on neural network algorithms, must be used [9, 10]. The most effective results are achieved by integrating these approaches with empirical data based on a comprehensive overview of real judicial and investigative practice for crimes of the type in question.

In the subsequent step of defining the tasks for computer modeling of digital rights crimes, we explore the possibilities of implementing a system of rules developed by owners of various information systems into the existing legal framework. However, this step introduced more uncertainties as formalizing these rules often revealed inconsistencies with the requirements of current legislation, particularly concerning the rules of international information systems used by Russian digital rights subjects for specific transactions.

To minimize the introduction of excessive uncertainty, it is advisable to form a second layer of the legal field, independent of the first, reflecting the characteristics of the formalized rules established for digital rights subjects by the owners of various types of Russian information systems. For the same reasons, a third layer of the legal field based on the formalized rules of international information systems used by Russian entities is also recommended. The fourth layer of the legal field can be developed by examining and summarizing aspects of criminal law norms applicable to crimes of the type under consideration, incorporating empirical data from judicial and investigative practices. This multilayered representation of the legal field offers a clearer view of the legal regulations governing the activities of digital rights subjects.

Furthermore, combined approaches for defining tasks for computer modeling of criminal manifestations in

the digital rights domain aim to harness the information capabilities of "empirical" and "theoretical" methods. By using the "multi-layered" characteristics of the existing legal field, they enhance the efficiency of such modeling while eliminating the challenge based on empirical data, those crime models in the digital rights field that violate fundamental principles of Russian criminal law.

At the stage of developing methods for solving problems related to computer modeling of possible criminal manifestations in the digital rights system, several options are available. The formation of a "multilayered" legal field provides an information and technological foundation for examining the characteristics of its components and their interrelationships, significantly reducing the number of provisions in current legislation whose convolution allows for the identification of elements in the committed crime. Within the corresponding algorithms, the following "localized" operations can be conducted:

1. Identification of possible violations of the rules of foreign information systems: a) by owners of information systems; b) clients of these information systems; and c) third parties.

2. Identification of possible violations of the requirements of current legislation by subjects of digital rights: a) by owners of information systems; b) clients of these information systems; and c) third parties.

3. Identification of possible violations of the rules of Russian information systems: a) by owners of information systems; b) clients of these information systems; and c) third parties.

4. Identification of possible inconsistencies between the rules of information systems of other countries and those of Russian information systems.

5. Identification of other possible violations and inconsistencies, depending on the specific situation related to the modeling of a specific crime in the field of digital rights.

It is important to clarify that these described theoretical approaches to computer modeling aim not so much at identifying possible violations of current legislation by digital rights subjects but at identifying potential sources of criminal manifestations within the digital rights domain. Consequently, the structure of the corresponding algorithms uses problem-oriented information processing systems and several criminal law criteria. Additionally, cyclic information processing plays an important role, allowing for the refinement of results through a series of successive approximations.

It is crucial to emphasize that approaches for establishing criteria of a criminal legal nature are not purely theoretical but are closely related to law enforcement practices in digital rights crimes. They aim to identify potential elements of such crimes by examining anomalies in the activities of digital rights subjects and exclude scenarios that do not constitute crimes. This involves the use of legal algorithms for "interval assessments" of the potential elements of crimes in the category.

Regarding the results of computer modeling of criminal manifestations in the digital rights domain that remain after the exclusion process, the methods used for their further processing are focused on significantly narrowing the intervals for each characteristic of potential crime elements and identifying the maximum number of mandatory and optional elements of such crimes. Empirical data from judicial and investigative practices are also integrated into this process.

Additionally, new algorithms for using the results of computer modeling of criminal manifestations in the digital rights field are emerging. By comparing the substantive features of "model" and "empirical" versions of crimes in this category with archived criminal cases that were previously suspended, opportunities arise for identifying the root causes of unusually high latency in certain types of digital rights crimes. This is particularly relevant to crimes associated with market manipulation, as mentioned earlier [1, 2].

A noteworthy aspect that deserves specific attention is the newfound potential of the developed algorithm system for computer modeling of criminal manifestations in the digital rights domain. An examination of the characteristics of criminal law norms for many types of such crimes reveals that, when forming their dispositions, the legislator did not pay adequate attention to their "processability" in law enforcement. This means that investigators must not only reveal the aspects of blanket, reference, and mixed dispositions within these criminal law norms but also address the problems of properly applying criminal-procedural norms to gather evidence from electronic documents and other electronic information.

Despite the proclaimed close connection between criminal and criminal-procedural law by many experts [11], real-world situations often give rise to various inconsistencies. Specifically, the interactions of digital rights subjects are documented in electronic documents created using specific software, including computer codes stored in relevant information systems. Some of these electronic documents may contain encoded traces of the crimes in question, which investigators must identify and document, while others may contain information relevant to the ongoing criminal investigation.

DOI: https://doi.org/10.17816/RJLS568994

Article 474.1 of the Code of Criminal Procedure of the Russian Federation (CCP RF) titled "Procedure for the use of electronic documents in criminal proceedings", introduced in 2016, primarily governs the submission of petitions, statements, complaints, and other electronic documents in court proceedings. However, there are currently no articles in the CCP RF that regulate the use of electronic documents in pre-trial proceedings or provide guidance to investigators on how to handle electronic documentation while generating evidence in a criminal case. This omission significantly complicates the proper implementation of investigative actions that involve electronic documents and other electronic information, which are essential for generating the necessary evidence and supporting relevant criminal cases in the field of digital rights.

The application of the aforementioned algorithms for computer modeling of criminal manifestations in the digital rights domain should not be limited exclusively to tasks directly linked to criminal law. If these algorithms are used to identify all the elements of specific digital rights crimes, a significant portion of the criminal legal problem can be addressed. However, if investigations are unable to effectively process large volumes of electronic documents to generate the required body of evidence in the relevant criminal cases, the primary goal of establishing a system for the criminal legal protection of digital rights subjects remains unsolved.

As previously mentioned, the use of sets of empirical data from judicial and investigative practices is integral to solving the first part of the problems related to computer modeling of criminal manifestations in this domain. This approach allows for the extraction and summarization of detailed criminal legal characteristics of digital rights crimes as determined by the court in the relevant criminal cases. Equally important is the examination and generalization of information related to the procedures for obtaining, verifying, and examining evidence in cases considered by the court. This information can be used to address the second set of tasks for computer modeling of criminal manifestations in the digital rights domain. This information can also be used to solve these problems within the framework of computer modeling.

While the first part of the computer modeling problem focused on the concept of "crime" as a key notion, the second part centers on the concept of "evidence". Through the examination of provisions such as Articles 17, 24, 73, and 74 of the CCP RF, as well as various other CCP RF provisions, the primary informational, criminal legal, and criminal-procedural aspects of this concept of "evidence" were established. This laid the foundation for the development of legal algorithms designed to process electronic and other information, to systematically obtain information that confirms the presence of elements of a specific digital rights crime in the act and supports circumstances that must be proven during the criminal investigation.

This approach allows for the integration of both the first and second parts of the identified problems related to computer modeling of criminal manifestations in the digital rights domain. The first part of the developed algorithm system focuses on the formalization of the characteristics of a specific crime within this domain. The second part is geared toward identifying encoded information traces of such crimes, generating the necessary evidence for relevant criminal cases, and conducting their verification and examination. In essence, this approach merges the essential aspects of the concept of "crime" as expounded in the General Part of the CC RF with the fundamental features of the concept of "evidence" as disclosed in the CCP RF.

As a result, the setting of computer modeling tasks for criminal manifestations in the digital rights domain entails the convergence of key concepts from criminal and criminal-procedural law, along with the associated provisions in the current legal framework. This involves not only the aforementioned articles of the CC RF but also several other provisions within these codes. The joint application of tools from criminal law to develop information support for investigative actions to reveal, disclose, and examine economic crimes was first documented in a book authored by a substantial team of scholars and practitioners [3].

Subsequently, algorithms for establishing the facts of problems, obtaining the necessary evidence, and conducting verification and examination, were developed and significantly expanded upon in a book produced at the Moscow Academy of the Investigative Committee of the Russian Federation [12]. These algorithms are not only applicable for proper verification and examination of individual pieces of evidence in specific criminal cases but also for determining the sufficiency of the cumulative evidence collected. This offers a fundamentally new approach to determining the limits of evidence in criminal cases related to digital rights crimes under investigation.

Thus, it can be affirmed that the approaches and methods for computer modeling of criminal manifestations in the digital rights domain presented here include several problems associated with establishing a modern system for the criminal legal protection of the rights and legitimate interests of citizens, organizations, the state, and society

as a whole during the era of universal computerization and digitalization. These methods are not only concerned with the timely detection of crimes of this nature and ensuring the inevitability of punishment for offenders but also focus on crime prevention.

It is worth noting that the practical application of the described algorithms for information and legal examination within the scope of computer modeling of the aforementioned criminal manifestations is a highly complex and labor-intensive task. Therefore, they need to be organized into a certain hierarchical system with cyclic application, using the principle of successive approximations, starting with the simplest analysis options based on specially generated criminal law criteria. Similar hierarchical algorithm systems have been outlined for various areas of developing and implementing methods for investigating various types of digital rights crimes, involving both the "traditional" and digital economies [13].

It is crucial to emphasize that the system of legal algorithms described here, which enables the simulation of intricate social processes characteristic of the transition to a new information society, falls within the scope of problems considered within the framework of cybernetics. This field, established in the late 1940s by the scientific group of Wiener and von Neumann, is based on the similarities between control and communication processes in machinery, living organisms, and their populations. Its primary goal is to explore the fundamental patterns that underlie control processes in various environments, conditions, and fields of human activity [14].

Primarily, this pertains to the processes of transmitting, storing, and processing information, the management of which occurs in complex dynamic systems characterized by variability and potential for development. These are attributes shared by the system of relationships in the digital rights domain. Problems associated with studying systems and resolved through mathematical methods. In essence, this entails the use of a specialized mathematical language, a language only comprehended by a few legal professionals.

The primary methods of cybernetics include algorithmization, the use of feedback, machine experiments, systems approach, and formalization. One of the most important achievements of cybernetics is the development of a method for mathematical modeling, where experiments are conducted not with a real physical model but with computer implementation of a mathematical model of the object under study, constructed according to its description. This approach offers significant flexibility when conducting experimental research.

This is precisely the situation typical of modeling social processes associated with the activities of subjects of digital rights, both law-abiding and others. Simultaneously, it pertains to a complex system of restrictions imposed on the activities of these entities by current legislation. In addition, this system of restrictions contains various gaps and contradictions that create conditions for various types of offenses and crimes. Identifying these problems based on the results of computer modeling will enable us the substantiate proposals for introducing appropriate changes and additions to the current legislation.

Moreover, after preparing and justifying such proposals, a new cycle of computer modeling can be conducted to create an "improved" system of legal regulation of the activities of digital rights subjects. If new problems are identified, it is possible to prepare new, more advanced, and better-substantiated options for changes and additions to the current legislation.

The theoretical foundation of cybernetics is mathematical cybernetics, which incorporates various branches of mathematics, including mathematical logic, discrete mathematics, probability theory, computational mathematics, information theory, coding theory, numbers theory, automata theory, complexity theory, mathematical modeling, and programing. Additionally, cybernetics involves various subfields such as technical, economic, biological, medical, physiological, and linguistic cybernetics. Each of these fields has its terminology, a distinct language with a specific set of concepts and operations that requires specialized training for mastery [14].

An analysis of the current situation regarding the establishment of a system for the criminal legal protection of subjects of digital rights reveals that the aforementioned approaches to creating hierarchical systems of algorithms for modeling crimes should be viewed as an initial step in the development of a new field of science, "juridic cybernetics". The creation of this field will involve resolving numerous problems and overcoming significant obstacles. One of the most pressing tasks is the development of a new legal algorithmic language with a carefully structured system of concepts and formalized connections within the appropriate thesaurus.

This endeavor will not only facilitate mutual understanding and effective collaboration between representatives of the criminal law and information fields but also address the uncertainties that often arise in communication among legal scholars, especially when they come from different legal specialties and scientific backgrounds. It is not without reason that the popular expression suggests that within a discussion between two

DOI: https://doi.org/10.17816/RJLS568994

lawyers, three opinions usually emerge. However, when an algorithmic language is used and the initial is informed, an unambiguous conclusion can be obtained. As the source data changes, a different but also unambiguous conclusion can be obtained.

Moreover, it is crucial to highlight the emergence of fundamentally new opportunities for the development of "legal cybernetics" at the intersection with the already established and successfully thriving field of linguistic cybernetics. Within the latter, not only are machine translation systems being developed but also serve as means of human-computer communication, including "natural" language, as well as structural models for processing, analyzing, and examining information. Consequently, regarding the practical implementation of the approaches, models, and algorithms described above, aimed at creating a system for the criminal legal protection of subjects of digital rights, a solid foundation already exists for the creation of modern tools.

In this context, it is imperative to revisit the statement made at the beginning of this article, which indicates that the legislator classifies the system of digital rights as rights of obligation. This underscores the need to prioritize the substantive features of obligations and rights of claim outlined in the contracts between information system owners and their clients. Within the framework of "smart contracts", these substantive features are concealed using blockchain technology not only from third parties but also from law enforcement agencies and courts. Therefore, if, during the conclusion of such a contract, a more experienced party decides to deceive the other party for its benefit, the deceived party's pursuit of the legal protection of its rights and legitimate interests appears to be exceedingly problematic.

Particularly challenging situations arise when subjects of digital rights must establish legal relationships with the owners of multiple information systems that may also have certain contractual relationships. Typically, these systems do not disclose their characteristics to their clients, resulting in a complex chain of obligations in which the interests of a specific client are not given primary consideration.

It is essential to note that the criminalization of acts in the field of rights of obligation has occurred in a rather contradictory manner. Following the introduction of Article 159.4 of the CC RF, "Fraud in business activities", in 2012, it was declared unconstitutional and became invalid in 2016. While some provisions related to deliberate failure to fulfill contractual obligations were introduced in the same year in parts 5, 6, and 7 of Article 159 of the CC RF "Fraud", they are still rarely applied in the field of digital rights.

This situation is particularly relevant to criminal manifestations associated with market manipulation, which are characterized by a high level of concealment, as mentioned earlier. Most of these crimes involve digital documentation circulated within interconnected information systems. According to current legislation, issue-grade securities are issued in the form of electronic records in certain information systems, and electronic exchange trading is conducted using other information systems. Transactions concluded through these systems are registered in the electronic registers of specialized information systems, and payments are made using electronic payment systems.

Moreover, the owners of these information systems generally use proprietary software and do not disclose the specifics of their contractual relationships to third parties. Criminals, however, exploit the most advanced information technologies to infiltrate one of the links in the described chain of information systems and take special measures to conceal their operations.

To identify and document traces of these types of crimes within the digital rights system, an extensive set of information technologies and problem-oriented software tools must be developed. Equally important is the development of well-founded proposals for the necessary changes and additions to criminal and criminal-procedural legislation. Achieving this requires computer modeling of criminal manifestations against the subjects of digital rights described, as described in this article, particularly in the context of market manipulation.

It is worth emphasizing that one of the most significant achievements of cybernetics is the identification and formulation of the problem of modeling human thinking processes. These problems take on a new significance in the context of modeling the thought processes of digital rights subjects, including their criminal aspects, as well as the thinking of lawyers working on establishing a system for criminal legal protection of these subjects. Furthermore, the use of the algorithms described above for information support of investigative actions offers fundamentally new opportunities for revealing the basic principles of criminal and criminal-procedural law in the evolving landscape of the information society.

For example, the implementation of one of the basic principles of criminal procedure law, as expressed in Article 17 of the CCP RF, "Freedom of evaluation of evidence", entails the formation of internal convictions among investigators, prosecutors, judges, and jurors. This formation is not based on the law and conscience but on the totality of evidence available in a criminal case. In actual

practice, many investigators struggle to pinpoint the specific legal guidelines they follow, and subjective examination exerts a significant influence when using the collected body of evidence to form an internal conviction.

This often leads to discrepancies in the examination of the results of the collected evidence between the investigator and prosecutors, prosecutors and the court, especially when jurors are involved. Due to the high degree of subjectivity in examining evidence, these situations often become difficult to resolve. Such discrepancies and conflicts do not contribute positively to the administration of justice in criminal cases involving new types of digital rights crimes.

Simultaneously, with the use of the system legal algorithms under consideration, several fundamentally new opportunities are created not only for shaping investigators' internal beliefs. The application of the provisions of criminal and criminal-procedural law to establish quantitative indicators of the sufficiency of the collected, properly verified, and examined body of evidence forms the basis for uniform approaches for informing all parties involved. This significantly helps in reducing the cases of disparities in examination results and, more importantly, conflict arising from differences in their approaches to forming internal convictions.

Here, it is important to address language and thinking problems, which are closely interconnected, especially when initiating the thought process of relevant individuals and forming its results. It is important to consider the similarities and fundamental differences in the language and thinking of the majority of digital rights subjects, criminal actors, and lawyers in the fields of lawmaking and enforcement.

The advancement of cybernetics and the emergence of computer science as a new science, involving a wide range of industry areas, poses new challenges to legal sciences. To accommodate the modern developments and interaction of computer science, mathematics, and cybernetics, it is important to determine acceptable methods for implementing the tools created in these fields in the field of criminal law sciences. This approach enables detailed research on the designated approaches, methods, and algorithms for computer modeling of criminal manifestations in the digital rights domain while avoiding purely "technocratic" solutions to complex legal problems.

The detailed development of the hierarchical systems of algorithms described earlier for computer or computer modeling of various aspects of social relations concerning digital rights enables the creation of the necessary software for practical application. This software can be divided into several packages designed for various purposes, with a focus on its interactive mode.

This software can be used to establish a set of "information standards" for legal relations among law-abiding subjects regarding digital rights in various economics, finance, management, and information exchange spheres. During its creation, hypertext technologies and other elements of AI can be used to select the most typical standards.

Software with a similar number of information processing algorithms can aim to develop "information standards" for unlawful conduct by subjects of digital rights. The selection of the most typical standards should take into account the specific features of the chains of obligatory rights of subjects with various levels and types. Using these standards, "information images" of not only the most common offenses in the digital rights domain can be formed. By comparing them with empirical data from judicial and investigative practice, sets of characteristics can be identified, and information standards can be formed for actually committed. This enables the initiation of new cycles of computer modeling in an interactive mode to create information images of sets of characteristics of these crimes.

These software packages are primarily intended for scientists and specialists involved in computer modeling of criminal manifestations in the digital rights domain. They are designed for interactive use, with results guiding users to conduct increasingly in-depth examinations, leading to a higher level of research problem formulation. This dialogue with a computer equipped with these programs occurs cyclically, allowing researchers to ascend to new levels of knowledge.

With a degree of convention, their activities can be described as "computer criminology" in the digital rights domain, as the results of such research can justify proposals for necessary changes and amendments to current criminal and criminal-procedural legislation.

Furthermore, based on the algorithms described above, packages of application software can be developed to provide information support for investigators, legal professionals, forensic experts, and specialists. Their specificity nature also involves interactive use, where legally significant decisions are made exclusively by authorized lawyers who enter relevant input data into the interactive forensic or expert system as needed in dialogue with their computer.

It is important to emphasize that when using many "branded" computer programs from foreign manufacturers, law enforcement officers often have to operate with an element of uncertainty due to the lack of complete disclosure regarding the system of algorithms on which these programs

DOI: https://doi.org/10.17816/RJLS568994

are built. As a result, it is common for programs to be based on the basic tenets of the Anglo-Saxon legal system, which may not align with the Russian legal system.

Unfortunately, such problems are often identified too late in the investigation process when the criminal case is already undergoing review by prosecutors or the court. Even when using similar software from Russian computer companies, it remains challenging to change the current situation based on the analysis results.

However, the detailed development of the hierarchical systems of algorithms described above enables a detailed description accessible to all participants in criminal proceedings. This requires the necessary "transparency" of the software built on these systems. Consequently, the information obtained through these computer programs can be adequately verified, as well as the evidence generated based on them in relevant criminal cases.

The practical implementation of the described set of studies in the field of computer modeling of criminal manifestations in the digital rights domain necessitates significant organizational efforts, and material and personnel support. A similar conclusion can be drawn regarding developments aimed at creating the necessary package of application software. These problems, including the possible establishment of a dedicated Center for scientific and technological research and development in the digital rights domain, have been discussed in our previous publications [15, 16].

Nevertheless, the primary objectives in the field of computer modeling of criminal manifestations in the digital rights domain remain centered on the detailed development of appropriate approaches and methods for creating algorithms of various types to process a wide range of information related to the formalization of the elements of the crimes in question, as well as their timely identification, disclosure, and investigations. Colleagues interested in discussing and addressing these issues are encouraged to also submit their proposals.

REFERENCES

1. Uroki pravoprimenitel'noi praktiki bor'by s manipulirovaniem rynkom. Nauchno-prakticheskoe posobie. Ed. by A.P. Opal'skii. Moscow: Al'pen-Print; 2022. (In Russ.).

2. Prorvich VA, Opal'skii AP, Ivanov EV, et al. Osobennosti ugolovno-pravovoi kharakteristiki prestuplenii, svyazannykh s manipulirovaniem rynkom: nauchno-prakticheskoe posobie. Moscow: Al'pen-Print, 2021. (In Russ.).

3. Organizatsiya i metodika rassledovaniya otdel'nykh vidov ekonomicheskikh prestuplenii. Ed. by A.I. Bastrykin, A.F. Volynskii, V.A. Prorvich. Moscow: Sputnik+; 2016. (In Russ.).

4. Oshibki pri raskrytii i rassledovanii ekonomicheskikh prestuplenii (vyyavlenie, ispravlenie i profilaktika). Ed. by A.I. Bastrykin, A.F. Volynsk, V.A. Prorvich. Moscow: Sputnik+; 2018. (In Russ.).

5. Gaukhman LD. Kvalifikatsiya prestuplenii: zakon, teoriya, praktika. Moscow: ZAO «YurInfoR»; 2013. (In Russ.).

6. Brychkov YuA. Integral'noe preobrazovanie. In: Bol'shaya Rossiiskaya Entsiklopediya. Vol. 11. Moscow: Bol'shaya Rossiiskaya Entsiklopediya; 2008. P. 425–426. (In Russ.).

7. Khvedelidze BV. Integral'noe uravnenie / Bol'shaya Rossiiskaya Entsiklopediya. Vol. 11. Moscow: Bol'shaya Rossiiskaya Entsiklopediya; 2008. P. 426–427. (In Russ.).

8. Timoshenko AA, Feizov VR, Chernov IV. Stsenarnyi podkhod k issledovaniyu napravlenii regulirovaniya sfery kriptovalyut v Rossiiskoi Federatsii. *Rossiiskii zhurnal pravovykh issledovanii.* 2023;10(2):21–30. (In Russ.).

9. Prorvich VA. Iskusstvennyi intellekt v sisteme ugolovno-pravovoi zashchity sub"ektov tsifrovykh prav. In: Sovetskaya i rossiiskaya kriminalistika: traditsii i perspektivy. Materialy vserossiiskoi nauchno-prakticheskoi konferentsii s mezhdunarodnym uchastiem (Moskva, 2 fevralya 2023 g.). Moscow: Moskovskaya akademiya Sledstvennogo komiteta Rossiiskoi Federatsii; 2023. P. 184–191. (In Russ.).

10. Bychkov VV, Prorvich VA. Iskusstvennyi intellekt v bor'be s ekstremizmom. *Rossiiskii zhurnal pravovykh issledovanii.* 2020;7(4):9–18. (In Russ.).

11. Kurs ugolovnogo protsessa. Ed. by L.V. Golovko. Moscow: Statut; 2016. (In Russ.).

12. Novikov AM, Prorvich VA. Dokazatel'stva i dokazyvanie v sledstvennoi praktike: uchebnoe posobie. Moscow: Moskovskaya akademiya Sledstvennogo komiteta Rossii; 2022. (In Russ.).

13. Volynskii AF, Prorvich VA. Komp'yuternaya kriminalistika v sisteme ugolovnopravovoi zashchity «traditsionnoi» i tsifrovoi ekonomiki: monografiya. Moscow: Ekonomika; 2020. (In Russ.).

14. Zhuravlev YuI., Gurevich IB. Kibernetika. In: Bol'shaya Rossiiskaya Entsiklopediya. Vol. 13. Moscow: Bol'shaya Rossiiskaya Entsiklopediya; 2009. P. 629–630. (In Russ.).

15. Prorvich VA. Osobennosti transfera informatsionnykh tekhnologii dlya formirovaniya kriminalisticheskogo instrumentariya po prestupleniyam v sfere tsifrovykh prav. Kriminalistika: nauka, praktika, opyt. Sbornik nauchnykh trudov Vserossiiskoi nauchno-prakticheskoi konferentsii. Moscow; 2022. P. 68–74. (In Russ.).

16. Prorvich VA. Informatsionno-metodicheskoe obespechenie ekspertno-kriminalisticheskoi deyatel'nosti po prestupleniyam v sfere tsifrovykh prav. In: Obshcheteoreticheskie problemy kriminalistiki i sudebnoi ekspertizy: sbornik materialov Mezhdunarodnogo nauchno-prakticheskogo foruma – kruglogo stola, posvyashchennogo pamyati V.Ya. Koldina, doktora yuridicheskikh nauk, Zasluzhennogo yurista RF, Zasluzhennogo deyatelya nauki RF, Zasluzhennogo professora Moskovskogo Universiteta (Moskva, 20 aprelya 2023 goda). Moscow: Izdatel'stvo Moskovskogo Universiteta; 2023. P. 174–181. (In Russ.).

СПИСОК ЛИТЕРАТУРЫ

1. Уроки правоприменительной практики борьбы с манипулированием рынком. Научно-практическое пособие / под. ред. А.П. Опальского. Москва: Альпен-Принт, 2022.

2. Прорвич В.А., Опальский А.П., Иванов Е.В., и др. Особенности уголовно-правовой характеристики преступлений, связанных с манипулированием рынком: научно-практическое пособие. Москва: Альпен-Принт, 2021.

3. Организация и методика расследования отдельных видов экономических преступлений / под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. Москва: Спутник+, 2016.

4. Ошибки при раскрытии и расследовании экономических преступлений (выявление, исправление и профилактика) / под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. Москва: Спутник+, 2018.

5. Гаухман Л.Д. Квалификация преступлений: закон, теория, практика. Москва: ЗАО «ЮрИнфоР», 2013.

6. Брычков Ю.А. Интегральное преобразование / Большая Российская Энциклопедия. Т. 11. Москва: Большая Российская Энциклопедия, 2008. С. 425–426.

7. Хведелидзе Б.В. Интегральное уравнение / Большая Российская Энциклопедия. Т. 11. Москва: Большая Российская Энциклопедия, 2008. С. 426–427.

8. Тимошенко А.А., Фейзов В.Р., Чернов И.В. Сценарный подход к исследованию направлений регулирования сферы криптовалют в Российской Федерации // Российский журнал правовых исследований. 2023. Т. 10. № 2. С. 21–30.

9. Прорвич В.А. Искусственный интеллект в системе уголовно-правовой защиты субъектов цифровых прав // Советская и российская криминалистика: традиции и перспективы. Материалы всероссийской научно-практической конференции с международным участием (Москва, 2 февраля 2023 г.). Москва: Московская академия Следственного комитета Российской Федерации, 2023. С. 184–191.

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

11. Курс уголовного процесса / под ред. Л.В. Головко. Москва: Статут, 2016.

12. Новиков А.М., Прорвич В.А. Доказательства и доказывание в следственной практике: учебное пособие. Москва: Московская академия Следственного комитета России, 2022.

13. Волынский А.Ф., Прорвич В.А. Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики. Москва: Экономика, 2020.

14. Журавлев Ю.И., Гуревич И.Б. Кибернетика / Большая Российская Энциклопедия. Т. 13. Москва: Большая Российская Энциклопедия, 2009. С. 629–630.

15. Прорвич В.А. Особенности трансфера информационных технологий для формирования криминалистического инструментария по преступлениям в сфере цифровых прав // Криминалистика: наука, практика, опыт. Сборник научных трудов Всероссийской научно-практической конференции. Москва, 2022. С. 68–74.

16. Прорвич В.А. Информационно-методическое обеспечение экспертно-криминалистической деятельности по преступлениям в сфере цифровых прав // Общетеоретические проблемы криминалистики и судебной экспертизы: сборник материалов Международного научно-практического форума — круглого стола, посвященного памяти В.Я. Колдина, доктора юридических наук, Заслуженного юриста РФ, Заслуженного деятеля науки РФ, Заслуженного профессора Московского Университета (Москва, 20 апреля 2023 года). Москва: Издательство Московского Университета. 2023. С. 174–181.

AUTHOR INFORMATION

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

ОБ АВТОРЕ

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

DOI: https://doi.org/10.17816/RJLS568994