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

ЭКО•ВЕКТОР

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

После введения в действующее законодательство Федеральным законом от 18.03.2019 № 34-ФЗ цифровых прав, которые законодатель отнес к имущественным правам, возникли новые проблемы, связанные с уголовно-правовой защитой субъектов таких прав, которыми становится большая часть граждан России. Их острота продолжает нарастать, но необходимые для этого уголовно-правовые и уголовно-процессуальные нормы до сих пор еще не приняты. Это вызывает «цепную реакцию» проблем и в правоприменении по соответствующим уголовным делам [1].

Наибольшие сложности правоприменения связаны с тем, что в соответствии с новой редакцией ст. 128 и ст. 141.1 ГК РФ цифровые права представляют собой «обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы». Но при введении нового правового понятия «правила информационной системы» законодатель не оговорил ни порядок их принятия, ни даже требование о необходимости соответствия таких правил требованиям действующего законодательства. А вопрос об ответственности за их нарушение «повис в воздухе».

Попытки толкования данных правовых норм «по умолчанию», учитывая, что все обладатели информационных систем являются законопослушными российскими гражданами, были опровергнуты самим же законодателем. При введении в действующее законодательство положений о цифровых финансовых активах Федеральным законом от 31 июля 2020 г. № 259-ФЗ было определено, что под цифровыми финансовыми активами понимаются цифровые права, выпуск, учет и обращение которых возможны только путем внесения записей в информационной системе на основе распределенного реестра. Они могут быть объектом залога, сделок купли-продажи, обмена одного вида цифровых финансовых активов на другой (в том числе выпущенных по ***правилам иностранных информационных систем***) или на цифровые права иных видов. Очевидно, что правила иностранных информационных систем создаются отнюдь не законопослушными российскими гражданами и «по умолчанию» не соответствуют требованиям действующего российского законодательства.

Оставляя в стороне вопросы защиты цифровых прав российских граждан в иностранных юрисдикциях, которые выходят за рамки настоящей статьи, важно обратить внимание на наиболее актуальные проблемы уголовно-правового характера. Отсутствие уголовно-правовых норм, раскрывающих особенности преступлений различного вида в сфере цифровых прав, приводит к новым проблемам, связанным с надлежащим раскрытием бланкетных диспозиций существующих уголовно-правовых норм. Именно здесь наиболее остро проявляется отсутствие законодательного регулирования правил информационных систем, устанавливающих порядок взаимодействия их обладателей со своими клиентами. Это создает ряд неопределенностей и при квалификации преступлений данного вида, что негативно влияет и на организацию их выявления, раскрытия и расследования [1, 2].

Проведенные исследования показывают, что процедуры раскрытия бланкетных, отсылочных и смешанных диспозиций уголовно-правовых норм с последующим формированием развернутых уголовно-правовых характеристик конкретных видов экономических преступлений отличаются высокой трудоемкостью [3]. Это связано, прежде всего, с тем, что следователю приходится учитывать особенности не только многочисленных положений десятков федеральных законов, но и сотен подзаконных актов различного уровня. К ним законодатель добавил еще и правила информационных систем, в рамках которых осуществляются самые различные транзакции в сфере цифровых прав. В результате возникает высокий уровень рисков совершения юридических ошибок — как по объективным, так и по субъективным причинам, но ответственность за их совершение ложится на следователя [4].

Среди объективных причин возникновения подобных юридических ошибок следует выделить явные недостатки в самих подходах, обозначенных многими учеными и специалистами в сфере уголовного права, на основе которых производится раскрытие бланкетных диспозиций уголовно-правовых норм по преступлениям в сфере экономики. По ряду сложившихся стереотипов, алгоритм соответствующих следственных действий основан на применении вначале положений Общей части УК РФ, а затем — федеральных законов и подзаконных актов [5]. При этом особую роль играет контроль за тем, чтобы при формировании развернутой уголовно-правовой характеристики расследуемого преступления следователь не вышел за рамки уголовного права.

С юридической точки зрения такой подход вполне оправдан, несмотря на ряд возникающих проблем при его практической реализации, создающих высокий уровень рисков совершения юридических ошибок. Но с математической точки зрения он означает, что следователю фактически приходится решать «обратную задачу». Ведь при разработке уголовно-правовой нормы законодателю нужно учитывать не только особенности тех общественных отношений, на которые посягают преступники. Принимаются по внимание и особенности гражданского и специального законодательства, регулирующего правоотношения в соответствующих сегментах общественных отношений экономических субъектов, и даже обычаи делового оборота.

Более того, при формировании некоторых уголовно-правовых норм по преступлениям в сфере цифровых прав законодатель уже начал использовать достаточно сложные математические модели вероятностного характера. При раскрытии их бланкетных диспозиций возникает ряд сложных проблем с идентификацией признаков объекта

и предмета преступления, а также его объективной стороны. Из-за этих, а также ряда других факторов объективного и субъективного характера отмечается аномально высокий уровень латентности таких преступлений. Прежде всего, речь идет о широком спектре преступных проявлений в сфере цифровых прав, связанных с манипулированием рынком [1, 2].

Соответствующие характеристики объекта преступления, раскрываемые учеными-криминологами, применительно к сфере цифровых прав требуют выполнения не только социологических исследований, но и раскрытия принципиально новых аспектов правоотношений в условиях перехода к новому, информационному обществу. Исследования криминологов, позволяющие раскрыть особенности объективной стороны таких преступлений, а также их субъектов и субъективной стороны, становятся еще более актуальными. Но такие исследования требуют больших затрат времени и пока еще далеки от завершения. А математическое моделирование преступных проявлений в сфере цифровых прав в исследованиях криминологов используется явно недостаточно.

С точки зрения математики процесс правотворчества имеет определенное сходство со сверткой функций многих переменных либо формированием интегрального преобразования [6]. В результате такой «юридической свертки» многочисленных положений действующего законодательства получается весьма лаконичная формулировка бланкетной, отсылочной или смешанной диспозиции соответствующей уголовно-правовой нормы. А попытка раскрыть такую диспозицию и сформировать развернутую уголовно-правовую характеристику конкретного преступления в рамках того правового поля, в котором действуют субъекты цифровых прав, представляет собой «обратную юридическую задачу».

Более детальный анализ особенностей подобной «юридической свертки», характеризующей преступные проявления в системе цифровых прав, включая затронутые выше проблемы формирования правил информационных систем, приводят к ее дополнительному усложнению. Здесь уже можно провести определенные аналогии с формированием интегральных уравнений различного рода [7]. Из-за наличия ряда неопределенностей в левой и правой частях «юридического интегрального уравнения», оно имеет бесконечное множество решений. Поэтому возникает высокий уровень рисков совершения юридических ошибок при попытках адаптировать существующие уголовно-правовые нормы к системе цифровых прав.

В математике были развиты различные способы решения подобных обратных задач, включая применение методов последовательных приближений, на основе теоремы Фредгольма, и ряда других. Для «некорректно поставленных» из-за ряда неопределенностей обратных задач были развиты методы регуляризации, позволяющие получить «интервальные оценки», в пределах которых находится искомое решение. При этом важную роль играет использование априорной информации, что также позволяет провести определенные аналогии с работой следователя по формированию развернутой уголовно-правовой характеристики расследуемого преступления с учетом всей имеющейся в его распоряжении информации.

По мере расширения использования в современной экономике криптовалют различного вида возникают разные сценарии регулирования правоотношений субъектов различного вида и уровня [8]. При этом приходится учитывать и влияние на развитие каждого из сценариев преступных проявлений, а также применяемых мер для снижения их негативного влияния. Но из-за использования технологии блокчейн выявление и фиксация таких преступлений в сфере цифровых прав представляет собой трудноразрешимую задачу. Однако при расследовании совокупностей таких преступлений, совершенных до и после использования криптовалюты, решение задач по выявлению и фиксации закодированных информационных следов значительно упрощается. Во многих случаях речь идет и об интервальных оценках соответствующей информации о деятельности субъектов цифровых прав.

Однако по мере развития возможностей компьютерной техники все более широкое применение стали находить методы прямого численного моделирования для решения подобных задач. Изменяя исходные данные в левой части уравнения в заранее установленных пределах, в результате численного моделирования получали тысячи решений прямой задачи, которые затем сравнивались с правой частью уравнения для установления наилучшего совпадения с ней одного из них — искомого решения. В некоторых случаях применялись и более сложные алгоритмы, например, отбиралось несколько вариантов решения, которые дополнительно исследовались с учетом априорной информации, чтобы получить искомое решение.

Применяя определенную аналогию к «юридическому моделированию», которое фактически используется следователями при формировании развернутых уголовно-правовых характеристик конкретного преступления рассматриваемого вида, важно обратить внимание на ряд его особенностей. Прежде всего, такие особенности проявляются уже на уровне постановки этих задач, а также при разработке системы алгоритмов для их решения. Но процесс подобного «юридического моделирования» преступной деятельности пока еще формализован в явно недостаточной степени, из-за чего нередко совершаются юридические ошибки, негативно влияющие на весь процесс расследования уголовного дела.

Проведенные исследования позволяют обратить внимание на следующие особенности формализации основных этапов подобного моделирования. Прежде всего, в качестве базовых исходных данных должны быть заложены важнейшие положения, использованные законодателем при формировании понятия «преступление» в ст. 14 УК РФ, а также положения Общей части УК РФ, детализирующие характеристики всех его признаков.

При этом в качестве «информационных эталонов» может использоваться система обязательных и факультативных признаков составов наиболее типичных преступлений в сфере цифровых прав.

Для того чтобы обеспечить «технологичность» уголовно-правовой характеристики преступлений рассматриваемого вида в плане надлежащего расследования соответствующих уголовных дел, в качестве второго основополагающего понятия при формировании системы исходных данных для компьютерного моделирования преступных проявлений в сфере цифровых прав должна быть использована совокупность признаков понятия «доказательство». Соответственно, речь идет о двух частях сформированной совокупности задач компьютерного моделирования, нацеленного не только на формирование важнейших признаков состава преступления, обеспечивающего его надлежащую квалификацию, но и на расследование уголовных дел о преступлениях в сфере цифровых прав.

На уровне постановки обеих частей рассматриваемых задач по компьютерному моделированию возможных преступных проявлений в системе цифровых прав можно выделить несколько возможных вариантов, имеющих различное содержание. Среди них условно можно обозначить «эмпирические», «теоретические» и «комбинированные».

Эмпирические варианты могут быть сориентированы на имеющийся практический опыт по выявлению, раскрытию и расследованию преступлений данного вида. Применительно к преступлениям в сфере цифровых прав здесь приходится сталкиваться с весьма ограниченным количеством преступлений некоторых видов, по итогам расследования которых были вынесены обвинительные приговоры. Наибольшее количество соответствующих уголовных дел характерно для мошенничества с использованием электронных средств платежа (ст. 159^3 УК РФ), наименьшее — для манипулирования рынком (ст. 185^3 УК РФ) [1, 2].

При формализации всей совокупности сведений, содержащихся в данных уголовных делах, могут быть выделены и систематизированы характеристики признаков объекта, объективной стороны, субъекта и субъективной стороны составов преступлений различного вида в сфере цифровых прав. Это позволит после сопоставления их особенностей с содержанием диспозиций соответствующих уголовно-правовых норм установить подходы к раскрытию бланкетных, отсылочных и смешанных диспозиций, которые использовались судами. По результатам их анализа создаются возможности для того, чтобы сформулировать соответствующие рекомендации для отбора наиболее адекватных правоприменительной практике вариантов компьютерного моделирования преступлений данного вида.

Эти рекомендации, в первую очередь, предназначены для уточнения разработанных моделей и алгоритмов компьютерного моделирования преступлений различного вида в сфере цифровых прав. Но на их основе могут также разрабатываться и методические рекомендации для расследования соответствующих уголовных дел о преступлениях в сфере цифровых прав, включая формирование необходимых для этого криминалистических методик.

Теоретические варианты предполагают, прежде всего, формирование формализованных характеристик «правового поля», раскрывающих особенности взаимодействия законопослушных субъектов цифровых прав — как обладателей информационных систем, так и потребителей оказываемых ими услуг. Для этого возможно выполнить моделирование такого взаимодействия на основе совокупности положений действующего гражданского и специального законодательства, а также сложившихся обычаев делового оборота, и создать определенную совокупность «информационных эталонов» деятельности законопослушных субъектов в существующем правовом поле.

Вместе с тем проведенные исследования показывают, что здесь возникает ряд неопределенностей из-за наличия некоторых нестыковок положений различных видов законодательства, и прежде всего, на уровне подзаконных актов. Кроме этого, к ним добавляются и уже отмеченные выше нестыковки правил, устанавливаемых обладателями информационных систем различного вида, с положениями действующего законодательства. Они могут устраняться различными способами, в том числе с использованием эмпирических данных.

При анализе теоретических вариантов моделирования отклонений от «эталонной» деятельности законопослушных субъектов цифровых прав и раскрытии особенностей наиболее характерных нарушений требований действующего законодательства, нельзя забывать о ключевых положениях уголовного права. Далеко не каждое нарушение требований действующего законодательства субъектами цифровых прав имеет все признаки состава преступления. И прежде всего, речь идет о проблемах идентификации признаков субъективной стороны преступления — наличия умысла, характера поставленных целей и формы вины.

Моделирование данных признаков состава преступления характеризуется наличием наибольших неопределенностей. Для их раскрытия необходимо использование определенных подходов, развитых в сфере криминологии, а также элементов искусственного интеллекта на основе нейросетевых алгоритмов [9, 10]. Но наибольший эффект достигается при сочетании данных подходов с применением эмпирических данных, основанных на обобщении реальной судебной и следственной практики по преступлениям рассматриваемого вида.

На следующем шаге постановки задач компьютерного моделирования преступлений в сфере цифровых прав речь идет о выяснении возможностей имплементации в данное правовое поле системы правил, созданных

обладателями информационных систем различного вида. Здесь возникает значительно больше неопределенностей, поскольку при их формализации проявляется ряд несоответствий некоторых из них требованиям действующего законодательства. И в первую очередь, это касается правил иностранных информационных систем, используемых российскими субъектами цифровых прав для совершения определенных транзакций.

Во избежание внесения высокого уровня неопределенностей представляется целесообразным формирование второго слоя правового поля, независимого от первого и отражающего особенности формализованных правил, установленных для субъектов цифровых прав обладателями российских информационных систем различного вида и назначения. По тем же причинам целесообразно также сформировать третий слой правового поля на основе формализованных правил иностранных информационных систем, используемых российскими субъектами. Четвертый слой правового поля может быть сформирован на основе анализа и обобщения особенностей уголовно-правовых норм по преступлениям рассматриваемого вида, с учетом уже упоминавшихся эмпирических данных из судебной и следственной практики. Такая многослойная характеристика правового поля позволяет более наглядно представить особенности правовой регламентации деятельности субъектов цифровых прав.

Наконец, комбинированные варианты постановки задач компьютерного моделирования преступных проявлений в сфере цифровых прав нацелены на объединение информационных возможностей «эмпирических» и «теоретических» вариантов. Они позволяют повысить эффективность такого моделирования с использованием «многослойной» характеристики существующего правового поля, исключив на основе эмпирической информации те варианты смоделированных составов преступлений в сфере цифровых прав, которые выходят за рамки важнейших принципов российского уголовного права.

На уровне разработки методов решения задач по компьютерному моделированию возможных преступных проявлений в системе цифровых прав можно выделить следующие возможные варианты. Формирование «многослойного» правового поля позволяет создать информационно-технологическую основу для анализа особенностей его составляющих, а также характеристик взаимных связей между ними. Это позволяет существенно уменьшить количество вариантов тех совокупностей положений действующего законодательства, свертка которых позволяет идентифицировать признаки состава совершенного преступления. В рамках соответствующих алгоритмов могут выполняться следующие «локальные» операции.

1. Выявление возможных нарушений правил иностранных информационных систем: а) со стороны обладателей информационных систем; б) со стороны клиентов этих информационных систем; в) со стороны третьих лиц.

2. Выявление возможных нарушений требований действующего законодательства субъектами цифровых прав: а) со стороны обладателей информационных систем; б) со стороны клиентов этих информационных систем; в) со стороны третьих лиц.

3. Выявление возможных нарушений правил российских информационных систем: а) со стороны обладателей информационных систем; б) со стороны клиентов этих информационных систем; в) со стороны третьих лиц.

4. Выявление возможных несоответствий правил иностранных информационных систем правилам российских информационных систем.

5. Выявление иных возможных нарушений и несоответствий, в зависимости от конкретной ситуации, связанной с моделированием конкретного преступления в сфере цифровых прав.

Здесь сразу же необходимо оговорить, что описываемые теоретические варианты компьютерного моделирования нацелены не столько на выявление возможных нарушений действующего законодательства субъектами цифровых прав, сколько на установление возможных источников преступных проявлений в сфере цифровых прав. Поэтому в структуре соответствующих алгоритмов используются проблемно-ориентированные системы обработки информации, а также ряд критериев уголовно-правового характера. Кроме того, важную роль играет циклический режим обработки информации, позволяющий уточнять полученные результаты в рамках системы последовательных приближений.

Необходимо подчеркнуть, что подходы к формированию критериев уголовно-правового характера носят не только «теоретический» характер, но и теснейшим образом связаны с правоприменительной практикой по преступлениям в сфере цифровых прав. Они нацелены на идентификацию возможных признаков составов таких преступлений по результатам анализа выявляемых аномалий в деятельности субъектов цифровых прав и «отсеивание» тех вариантов правонарушений, которые преступлениями не являются. То есть речь идет о применении юридических алгоритмов для «интервальных оценок» признаков возможных составов преступлений рассматриваемого вида.

Что касается оставшихся после «отсеивания» результатов компьютерного моделирования преступных проявлений в сфере цифровых прав, то используемые методы их дальнейшей обработки сориентированы на существенное сужение интервалов характеристик каждого из признаков возможных составов преступлений и установление максимального количества обязательных и факультативных признаков составов возможных преступлений данного вида. Для этого также используются эмпирические данные из судебной и следственной практики.

В то же время возникают и принципиально новые варианты алгоритмов использования результатов компьютерного моделирования преступных проявлений в сфере

цифровых прав. По результатам сопоставления содержательных особенностей «модельных» и «эмпирических» вариантов составов преступлений рассматриваемого вида с архивными уголовными делами, расследование которых было приостановлено, возникает ряд возможностей для выявления причин аномально высокой латентности определенных видов преступлений в сфере цифровых прав. В первую очередь, это актуально для уже упоминавшихся выше преступлений, связанных с манипулированием рынком [1, 2].

Необходимо специально обратить внимание на еще одну принципиально новую возможность использования системы разрабатываемых алгоритмов для компьютерного моделирования преступных проявлений в сфере цифровых прав. Изучение особенностей уголовно-правовых норм по многим видам таких преступлений показывает, что при формировании их диспозиций законодатель не уделил необходимого внимания «технологичности» их правоприменения. То есть следователю приходится не только раскрывать особенности бланкетных, отсылочных и смешанных диспозиций данных уголовно-правовых норм, но и решать проблемы надлежащего применения уголовно-процессуальных норм при формировании доказательств на основе электронных документов и иной электронной информации.

Несмотря на декларируемую многими учеными неразрывную связь уголовного и уголовно-процессуального права [11], в реальной практике нередко возникают нестыковки различного рода. В частности, отношения субъектов цифровых прав отражаются в электронных документах, созданных с помощью определенного программного обеспечения — компьютерных кодов, хранящихся в соответствующих информационных системах. Некоторые из этих электронных документов содержат в себе закодированные информационные следы преступлений рассматриваемого вида, которые должен выявить и зафиксировать следователь. В других можно выявить информацию, имеющую значение для расследуемого уголовного дела.

Но ст. 474.1 УПК РФ «Порядок использования электронных документов в уголовном судопроизводстве», введенная еще в 2016 г., регламентирует только порядок подачи ходатайств, заявлений, жалоб и иных электронных документов в суд, а также получение судебных решений и их копий в виде электронных документов. В то же время статей, регламентирующих порядок использования электронных документов в досудебном производстве, а также порядок обращения следователей с электронной документацией при формировании доказательств по уголовному делу, в УПК РФ не имеется. Это существенно осложняет надлежащее выполнение следственных действий с использованием электронных документов и иной электронной информации, нацеленных на формирование необходимых доказательств и доказывание по соответствующим уголовным делам о преступлениях в сфере цифровых прав.

Применение описанных выше алгоритмов компьютерного моделирования преступных проявлений в сфере цифровых прав не должно ограничиваться только задачами, относящимися исключительно к сфере уголовного права. Если с их помощью будут идентифицированы все признаки составов конкретных преступлений в сфере цифровых прав, то значительная часть задач уголовно-правового характера может считаться решенной. Но если при этом следствие не сможет надлежащим образом обработать большие массивы электронных документов, чтобы сформировать необходимую и достаточную совокупность доказательств по соответствующим уголовным делам, то главная задача — создание системы уголовно-правовой защиты субъектов цифровых прав останется нерешенной.

Выше уже упоминалось об использовании в рамках решения первой части задач компьютерного моделирования преступных проявлений в данной сфере совокупностей эмпирических данных из судебной и следственной практики. Это означает, что из материалов соответствующих уголовных дел могут быть извлечены и обобщены не только установленные судом развернутые уголовно-правовые характеристики преступлений в сфере цифровых прав. Не меньшее значение для постановки второй группы задач по компьютерному моделированию преступных проявлений в сфере цифровых прав имеет анализ и обобщение сведений о процессе получения, проверки и оценки доказательств по уголовным делам, рассмотренных судом. Эти сведения могут использоваться и при решении данных задач в рамках компьютерного моделирования.

Если при постановке первой части задач компьютерного моделирования в качестве ключевого положения использовалось понятие «преступление», то для их второй части таким положением является понятие «доказательство». По результатам анализа совокупности положений ст. 17, 24, 73, 74 УПК РФ, а также ряда других положений УПК РФ были установлены основные информационные, уголовно-правовые и уголовно-процессуальные аспекты данного понятия. Это позволило разработать юридические алгоритмы обработки электронной и иной информации, нацеленные на получение в установленном порядке сведений, подтверждающих наличие в деянии признаков состава конкретного преступления рассматриваемого вида, а также обстоятельств, подлежащих доказыванию при расследовании уголовного дела.

Данный подход позволяет объединить первую и вторую части рассматриваемых задач компьютерного моделирования криминальных проявлений в сфере цифровых прав. При этом если первая часть разработанной системы алгоритмов позволит формализовать систему признаков состава конкретного преступления рассматриваемого вида, то вторая часть данной системы нацелена на выявление закодированных информационных следов преступлений данного вида и формирование необходимых

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

доказательств по соответствующим уголовным делам, а также выполнение их проверки и оценки. То есть важнейшие признаки понятия «преступление», раскрытые в Общей части УК РФ, соединяются тем самым с важнейшими признаками понятия «доказательство», раскрытыми в УПК РФ, а также в УК РФ.

Таким образом, в рамках постановки задач компьютерного моделирования криминальных проявлений в сфере цифровых прав фактически происходит объединение ключевых понятий уголовного и уголовно-процессуального права, а также соответствующих положений действующего законодательства. При этом речь идет не только об уже указанных выше статьях УК РФ и УПК РФ, но и о ряде иных положений данных кодексов. Описание подобного совместного применения инструментария наук уголовно-правового блока для разработки информационного обеспечения следственных действий по выявлению, раскрытию и расследованию экономических преступлений впервые было опубликовано в книге, подготовленной большим коллективом ученых и специалистов-практиков [3].

Позднее алгоритмы формирования предмета доказывания, получения необходимых доказательств, их проверки и оценки были развиты и существенно дополнены в книге, подготовленной в Московской академии Следственного комитета РФ [12]. С их помощью создается возможность не только для надлежащей проверки и оценки каждого из доказательств по конкретному уголовному делу, но и для установления достаточности собранной совокупности доказательств. Тем самым создаются и принципиально новые средства для установления пределов доказывания по расследуемым уголовным делам о преступлениях в сфере цифровых прав.

В итоге можно констатировать, что описанные подходы и методы компьютерного моделирования преступных проявлений в сфере цифровых прав позволяют охватить весь комплекс проблем, связанных с созданием современной системы уголовно-правовой защиты прав и законных интересов граждан, организаций, государства и общества в целом в переходных условиях ко всеобщей информатизации и цифровизации. При этом речь идет не только о своевременном выявлении преступлений рассматриваемого вида и обеспечении неотвратимости наказания преступников, но и о профилактике таких преступлений.

Проведенные исследования показывают, что практическая реализация перечисленных выше алгоритмов информационно-правового анализа в рамках компьютерного моделирования рассматриваемых преступных проявлений отличается высокой сложностью и трудоемкостью. Поэтому возникает необходимость выстраивания их в определенную иерархическую систему с циклическим применением, с использованием принципа последовательных приближений, начиная с наиболее простых вариантов анализа на основе специально сформированных уголовно-правовых критериев. Подобные иерархические системы алгоритмов были описаны применительно к ряду направлений создания и использования методик расследования различных видов преступлений в сфере цифровых прав, совершаемых как в рамках «традиционной», так и цифровой экономики [13].

Важно подчеркнуть, что описанная система юридических алгоритмов, позволяющая выполнить моделирование весьма сложных общественных процессов, характерных для перехода к новому, информационному обществу, полностью находится в сфере тех проблем, которые рассматриваются в рамках кибернетики. Ведь в основе данной науки, созданной в конце 40-х гг. прошлого века научной группой Винера — фон Неймана, лежит сходство процессов управления и связи в машинах, живых организмах и их популяциях, а ее основной задачей является исследование общих закономерностей, лежащих в основе процессов управления в различных средах, условиях, областях человеческой деятельности [14].

Прежде всего, речь идет о процессах передачи, хранения и переработки информации, управление которыми протекает в сложных динамических системах — объектах, обладающих изменчивостью и способностью к развитию. Именно такими свойствами обладает система отношений в сфере цифровых прав. А соответствующие задачи изучения систем и процессов управления ими, а также информационных процессов описываются и решаются математическими методами. То есть речь идет об использовании для этого специального, математического языка, которым владеют пока еще лишь немногие юристы.

К основным методам кибернетики относятся алгоритмизация, использование обратных связей, машинный эксперимент, системный подход, формализация и ряд других. Одним из важнейших достижений кибернетики является разработка метода математического моделирования, в рамках которого эксперименты производятся не с реальной физической моделью, а с компьютерной реализацией математической модели изучаемого объекта, построенной по его описанию. Это обеспечивает ее наибольшую гибкость при выполнении экспериментального исследования.

Именно такая ситуация характерна для описанной выше задачи моделирования социальных процессов, связанных с деятельностью субъектов цифровых прав — как законопослушных, так и иных. При этом речь идет о сложной системе ограничений, накладываемых на деятельность данных субъектов действующим законодательством. Кроме того, данная система ограничений имеет ряд пробелов и противоречий, которые создают условия для различного рода правонарушений и преступлений. Их выявление по результатам компьютерного моделирования позволит обосновать предложения по внесению соответствующих изменений и дополнений в действующее законодательство.

Более того, после подготовки и обоснования таких предложений возможно выполнить новый цикл компьютерного моделирования уже для «усовершенствованной» на их основе системы правового регулирования деятельности субъектов цифровых прав. В случае выявления

новых проблем возможно подготовить новые, более совершенные и лучше обоснованные варианты изменений и дополнений в действующее законодательство.

Здесь важно обратить внимание на то, что теоретическую основу кибернетики составляет математическая кибернетика, в рамках которой используются такие разделы математики, как математическая логика, дискретная математика, теория вероятностей, вычислительная математика, теория информации, теория кодирования, теория чисел, теория автоматов, теория сложности, математическое моделирование и программирование. При этом в кибернетике уже выделяется техническая, экономическая, биологическая, медицинская, психологическая, физиологическая, лингвистическая кибернетика. Каждая из этих наук имеет свой аппарат, специфический язык с определенной системой понятий и операций с ними, для овладения которым необходима специальная подготовка [14].

Анализ сложившейся ситуации в создании системы уголовно-правовой защиты субъектов цифровых прав показывает, что перечисленные выше подходы к созданию иерархических систем алгоритмов для моделирования преступлений следует рассматривать лишь как первый шаг в создании новой отрасли науки — «юридической кибернетики». Понятно, что для ее создания потребуется решить много проблем и преодолеть серьезные препятствия. И одной из наиболее актуальных задач становится создание нового, юридического алгоритмического языка, со специальным образом сформированной системой используемых понятий и формализованных связей между ними в соответствующем тезаурусе.

Это позволит не только обеспечить взаимопонимание, а затем и надлежащее взаимодействие представителей наук уголовно-правового и информационного блоков. Важным последствием его применения может стать устранение тех неопределенностей, которые нередко возникают при общении ученых-юристов, особенно если они представляют различные юридические специальности и научные школы. Отнюдь не случайно возникло крылатое выражение о том, что в рамках дискуссии двух юристов обычно вырабатывается три мнения. Но при использовании алгоритмического языка в результате преобразования исходной информации получается однозначный вывод. А при изменении исходных данных получается другой, но также однозначный вывод.

Важно обратить внимание и на то, что принципиально новые возможности для создания «юридической кибернетики» возникают на стыке с уже существующей и успешно развивающейся лингвистической кибернетикой. В рамках последней развиваются не только системы машинного перевода, но и средства общения человека с компьютером, в том числе на «естественном» языке, а также структурные модели обработки, анализа и оценивания информации. То есть применительно к практической реализации описанных выше подходов, моделей и алгоритмов, нацеленных на создание системы уголовно-правовой защиты субъектов цифровых прав, уже имеется серьезный задел для создания современного инструментария.

В этой связи необходимо вернуться к констатации в самом начале данной статьи о том, что система цифровых прав отнесена законодателем к обязательственным правам. Это требует уделения первоочередного внимания тем содержательным особенностям обязательств и прав требования, которые указываются в договорах между обладателями информационных систем и их клиентами. А в рамках «смарт-контрактов» эти содержательные особенности закрываются с помощью блокчейн-технологии не только от третьих лиц, но и от правоохранительных органов и судов. Поэтому если при заключении такого контракта одна, более опытная сторона решит обмануть другую сторону, исходя из своих интересов, то обращение обманутой стороны в суд для защиты своих прав и законных интересов становится весьма проблематичным.

Особенно сложные ситуации возникают в таких случаях, когда субъектам цифровых прав приходится вступать в правоотношения с обладателями нескольких информационных систем, которые связаны друг с другом также определенными договорными отношениями. Их особенности своим клиентам они, как правило, не раскрывают. Поэтому возникает достаточно сложная цепочка обязательственных прав, в рамках которой интересы конкретного клиента учитываются далеко не в первую очередь.

Здесь необходимо обратить внимание на то, что криминализация деяний в сфере обязательственных прав происходит весьма противоречиво. После введения в 2012 г. ст. 159.4 УК РФ «Мошенничество в сфере предпринимательской деятельности» она была признана неконституционной и утратила силу в 2016 г. Некоторые положения, связанные с преднамеренным неисполнением договорных обязательств, были в том же году введены в части 5, 6 и 7 ст. 159 УК РФ «Мошенничество». Но в сфере цифровых прав они применяются пока еще весьма редко.

Именно такая ситуация характерна для преступных проявлений, связанных с манипулированием рынком, высочайший уровень латентности которых уже отмечался выше. Большая часть преступлений рассматриваемого вида совершается с использованием документации в цифровой форме, которая обращается в нескольких взаимосвязанных информационных системах. В соответствии с действующим законодательством эмиссионные ценные бумаги выпускаются в бездокументарной форме электронных записей в определенных информационных системах, а электронные биржевые торги осуществляются с помощью других информационных систем. Заключенные сделки с ними регистрируются в электронных реестрах специализированных информационных систем, а платежи осуществляются с помощью электронных платежных систем.

При этом обладатели соответствующих информационных систем используют, как правило, оригинальное

программное обеспечение, а особенности своих договорных отношений третьим лицам не раскрывают. В то же время преступники применяют самые современные информационные технологии, внедряясь в одно из звеньев описанной цепочки информационных систем. Кроме этого, они применяют специальные меры для сокрытия своих операций.

Понятно, что для выявления и фиксации следов преступлений данного вида в системе цифровых прав необходима разработка обширного комплекса информационных технологий и проблемно-ориентированных программных средств. Не менее важна и разработка обоснованных предложений о внесении необходимых изменений и дополнений в уголовное и уголовно-процессуальное законодательство. А для этого необходимо выполнение описываемого в данной статье компьютерного моделирования преступных проявлений против субъектов цифровых прав в рамках манипулирования рынком.

Следует специально подчеркнуть, что одним из важнейших достижений кибернетики является выделение и постановка проблемы моделирования процессов мышления человека. Эти проблемы приобретают новый смысл в контексте моделирования мышления субъектов цифровых прав, в том числе и его криминальных аспектов, а также мышления юристов, создающих систему уголовно-правовой защиты данных субъектов. При этом использование описанных выше алгоритмов информационного обеспечения следственных действий создает принципиально новые возможности для раскрытия основных принципов уголовного и уголовно-процессуального права в контексте нового содержания отношений в информационном обществе.

К примеру, реализация одного из основных принципов уголовно-процессуального права, сформулированного в ст. 17 УПК РФ «Свобода оценки доказательств», предусматривает формирование внутреннего убеждения следователей, прокуроров, судей и присяжных заседателей не только на основе закона и совести. Речь идет об использовании для этого совокупности имеющихся в уголовном деле доказательств. В реальной практике многие следователи затрудняются в определении конкретного закона, которым они должны руководствоваться, а что касается использования для формирования внутреннего убеждения собранной совокупности доказательств по делу, то здесь отмечается существенное влияние субъективных оценок.

Нередко это приводит к противоречиям в результатах оценки собранной совокупности доказательств следователем и прокурором, прокурором и судом, особенно с участием присяжных заседателей. Более того, из-за высокой доли субъективизма в оценке доказательств со стороны указанных лиц нередко возникают сложно разрешимые конфликтные ситуации. Все это не идет на пользу отправлению правосудия по уголовным делам о новых видах преступлений в сфере цифровых прав.

В то же время с помощью рассматриваемой системы юридических алгоритмов создается ряд принципиально новых возможностей не только для формирования внутренних убеждений следователей. Применение положений уголовного и уголовно-процессуального права для установления количественных показателей достаточности собранной совокупности доказательств, прошедших надлежащую проверку и оценку, создает основы для применения единообразных подходов к информированию всех перечисленных выше лиц. Это во многом способствует устранению причин для возникновения противоречий в результатах их оценки, а тем более — конфликтных ситуаций из-за различий в подходах к формированию внутренних убеждений этих лиц.

Здесь также следует обратить внимание на уже отмеченные выше проблемы используемого языка, который тесно связан с мышлением, по крайней мере, при инициировании процесса мышления соответствующих субъектов, а также формировании его результата. При этом важно учитывать определенное сходство и принципиальные различия языка и мышления основной массы субъектов цифровых прав, криминальных элементов и юристов — как правотворцев, так и правоприменителей.

Развитие кибернетики и создание на ее базе новой науки — информатики, в рамках которой развивается широкий спектр отраслевых направлений, ставит новые задачи и перед юридическими науками. Учитывая современные особенности развития и взаимодействия основных школ информатики, математики и кибернетики, важно найти приемлемые способы имплементации созданного в рамках данных наук инструментария в сферу наук уголовно-правового блока. Это позволит не только развернуть соответствующие исследования по детализации обозначенных подходов, методов и алгоритмов компьютерного моделирования преступных проявлений в сфере цифровых прав, но и избежать чисто «технократических» подходов к решению сложных проблем правового характера.

Детальная разработка описанных выше иерархических систем алгоритмов компьютерного моделирования особенностей общественных отношений субъектов цифровых прав позволяет создать и необходимое программное обеспечение для их практического применения. При этом речь идет о нескольких пакетах прикладных программ различного назначения, сориентированных на их применение в интерактивном режиме.

В первую очередь, это программное обеспечение, позволяющее сформировать на основе анализа положений действующего законодательства определенную совокупность «информационных эталонов» правоотношений законопослушных субъектов цифровых прав в различных сферах экономики, финансов, управления, информационного обмена и т.п. При его создании могут быть использованы гипертекстовые технологии и другие элементы искусственного интеллекта, чтобы отобрать наиболее типичные из них.

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

Аналогичное по ряду использованных алгоритмов обработки информации программное обеспечение может быть нацелено на формирование «информационных эталонов» противоправного поведения субъектов цифровых прав. Отбор наиболее типичных из них должен осуществляться с учетом отмеченных выше особенностей цепочек обязательственных прав субъектов различного вида и уровня. С их использованием возможно формирование «информационных образов» не только наиболее распространенных правонарушений в сфере цифровых прав. По результатам их сопоставления с эмпирическими данными из судебной и следственной практики могут быть выявлены совокупности признаков и сформированы «информационные эталоны» реально совершаемых преступлений рассматриваемого вида. Это позволяет выполнить новые циклы компьютерного моделирования в интерактивном режиме для формирования «информационных образов» совокупностей характеристик составов таких преступлений.

Данные пакеты прикладных программ предназначены, прежде всего, для ученых и специалистов, занимающихся компьютерным моделированием криминальных проявлений в сфере цифровых прав. При этом речь идет об использовании этих программ в интерактивном режиме, когда полученные результаты ориентируют их пользователей на выполнение все более глубокого анализа с последующим переходом на более высокий уровень постановки исследовательских задач. Соответственно, подобный диалог с компьютером, оснащенным комплексом данных программ, продолжается в циклическом режиме, обеспечивая возможность восхождения исследователя на новые витки спирали познания.

С определенной долей условности их деятельность можно охарактеризовать как «компьютерную криминологию» в сфере цифровых прав, поскольку по результатам таких исследований могут быть обоснованы предложения о внесении необходимых изменений и дополнений в действующее уголовное и уголовно-процессуальное законодательство.

В то же время на основе описанных выше алгоритмов возможно также сформировать и пакеты прикладных программ, предназначенных для информационного обеспечения деятельности следователей, оперативных сотрудников, судебных экспертов и специалистов. Их спецификой также является интерактивный режим использования, в рамках которого процессуально значимые решения принимает только уполномоченный на выполнение соответствующих действий юрист. А с помощью программного обеспечения в диалоговом режиме со своим компьютером он получает необходимую ему информацию, вводя соответствующие исходные данные в соответствующую интерактивную криминалистическую или экспертную систему, а затем изменяя их по мере необходимости.

Здесь важно подчеркнуть, что при использовании многих видов «фирменных» компьютерных программ зарубежных производителей правоприменителям приходится действовать если не вслепую, то с элементами игры «веришь — не веришь». Это связано с тем, что полное описание системы алгоритмов, на основе которых написаны тексты таких программ, фирмы не раскрывают. Поэтому нередко оказывается, что в основу таких «фирменных» компьютерных программ заложены основные положения англо-саксонской правовой семьи, имеющие мало общего с российской правовой системой.

К сожалению, подобные проблемы системного характера во многих случаях выявляются слишком поздно для следствия, когда уголовное дело уже «разваливается» при его рассмотрении прокурором или судом. При этом, как показывают результаты проведенного анализа, изменить сложившуюся ситуацию, даже при использовании подобного программного обеспечения, созданного российскими компьютерными фирмами, крайне сложно.

В то же время детальная разработка описанных выше иерархических систем алгоритмов компьютерного моделирования преступных проявлений в сфере цифровых прав позволяет создать их подробное описание, доступное для всех участников уголовного судопроизводства. Это обеспечивает необходимую «прозрачность» создаваемого на их основе программного обеспечения. То есть те сведения, которые могут быть получены с помощью данных компьютерных программ, могут быть проверены надлежащим образом, как и сформированные на их основе доказательства по соответствующим уголовным делам.

Безусловно, практическая реализация описанного комплекса исследований в сфере компьютерного моделирования преступных проявлений в сфере цифровых прав требует серьезных организационных усилий, материального и кадрового обеспечения. Аналогичный вывод можно сделать и в отношении разработок, нацеленных на создание необходимого комплекса прикладного программного обеспечения. Соответствующие проблемы, включая возможное создание специального Центра научно-технологических исследований и разработок в сфере цифровых прав, а также основные способы их решения обсуждались в ряде наших других публикаций [15, 16].

Тем не менее первоочередными задачами в сфере компьютерного моделирования преступных проявлений в сфере цифровых прав остается детальная разработка соответствующих подходов и методов формирования алгоритмов различного вида для обработки обширного комплекса информации, связанной как с формализацией признаков составов совершаемых преступлений рассматриваемого вида, так и их своевременного выявления, раскрытия и расследования. Коллеги, заинтересованные в обсуждении и решении обозначенных проблем, могут направить свои предложения по адресу: kse60@mail.ru.

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

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.

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.).

ОБ АВТОРЕ

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

AUTHOR INFORMATION

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