Право. Журнал Высшей школы экономики. 2024. Том 17. № 2.
Law. Journal of the Higher School of Economics. 2024. Vol. 17, no 2.

Научная статья
УДК: 343.9
DOI:10.17323/2072-8166.2024.2.143.169

Информационные основы современной уголовно-правовой защиты субъектов цифровой экономики и финансов

Сергей Владимирович Расторопов[1], Владимир Антонович Прорвич[2]

[1, 2] Национальный исследовательский университет «Высшая школа экономики», Россия 101000, Москва, Мясницкая ул., 20,

[1] srastoropov@hse.ru https://orcid.org/0009-0005-8105-4514

[2] kse60@mail.ru htpps://orcid.org/0000-0000-5964-9056

Аннотация

Эффективность уголовно-правовой защиты субъектов цифровой экономики и финансов в значительной степени зависит от интегрированного применения инструментария, созданного в рамках наук уголовно-правового и информационного блоков. Важную роль в криминализации общественных отношений в сфере цифровых прав, которые активно используются киберпреступностью, играет компьютерное моделирование. Основные источники юридических ошибок при организации уголовно-правовой защиты субъектов цифровых прав возникают из-за попыток механического перенесения некоторых понятий из арифметики, физики, микроэлектроники и других естественных наук в сферу уголовного права. Законодатель связал понятия «цифровых прав» с новым правовым понятием «правил информационной системы». Такие правила создают обладатели информационных систем, а соответствующие правовые предписания на уровне федеральных законов отсутствуют. Вместе с тем взаимосвязанные информационные системы давно применяются при совершении биржевых транзакций с эмиссионными ценными бумагами, а нестыковки правил этих систем нередко приводят к юридическим ошибкам при выявлении криминальных событий. Для их профилактики предлагаются новые способы имплементации инструментария наук информационного блока в сферу уголовно-правовых наук. Одним из наиболее действенных является выделение из определенных совокупностей уголовно-правовых и граждан-

ско-правовых норм юридических алгоритмов, позволяющих сформировать развернутую уголовно-правовую характеристику конкретного киберпреступления и идентифицировать признаки его состава для надлежащей квалификации. Другие виды юридических алгоритмов позволяют идентифицировать особенности предмета и пределов доказывания по уголовному делу о киберпреступлениях рассматриваемого вида. Третьи — организовать применение методики расследования таких киберпреступлений в циклическом режиме с обратными связями для выявления каждого из преступлений и дифференциации их составов. Формирование иерархических систем юридических алгоритмов различного вида и назначения позволяет создать на их основе ряд проблемно-ориентированных компьютерных программ, обеспечивающих правоприменение интерактивных информационных систем для обработки электронных документов и иной информации при выявлении и раскрытии преступлений в сфере цифровой экономики и финансов.

Ключевые слова

киберпреступления; цифровая экономика и финансы; цифровые права; цифровые финансовые активы; манипулирование рынком; юридические алгоритмы; интерактивные информационные системы.

Для цитирования: Расторопов С.В., Прорвич В.А. Информационные основы современной уголовно-правовой защиты субъектов цифровой экономики и финансов // Право. Журнал Высшей школы экономики. 2024. Том 17. № 2. С. 143–169. DOI:10.17323/2072-8166.2024.2.143.169

Research article

Information Bases of Modern Criminal Law Protecting Subjects of Digital Economy and Finance

Sergey V. Rastoropov, Vladimir A. Prorvich

[1, 2] National Research University Higher School of Economics, 20 Myasnitskaya Str., Moscow 101000, Russia,

[1] srastoropov@hse.ru

[2] kse60@mail.ru

Abstract

The value of criminal law protecting digital economy and financial entities largely depends on the integrated application of tools created within the framework of the sciences of criminal law and information blocks. Computer modeling plays an important role in the proper criminalization of new social relations in the field of digital rights recently introduced into the current legislation, which are actively used by cybercrime of various types. The main sources of legal errors in the organization of criminal law protection of subjects of digital rights arise due to attempts to “mechanically” transfer some concepts from arithmetic, physics, microelectronics and other natural sciences

to the field of criminal law. Moreover, the legislator linked the concepts of “digital rights” with the new legal concept of “rules of the information system”. At the same time, that rules are created by the “owners” of information systems, and there are no relevant legal regulations on their structure and content at the level of federal laws. At the same time, interconnected information systems have long been used in making exchange transactions with equity securities, and non-alignment of the rules of these systems often lead to legal errors in identifying relevant criminal events. To prevent them, new ways of proper implementation of the tools of the information block sciences in the field of criminal law sciences are proposed. One of the most effective is the identification of legal algorithms from certain sets of criminal and civil law norms, which make it possible to form a detailed criminal law characteristic of a specific cybercrime and identify the features of its composition for proper qualification. Other types of legal algorithms make it possible to identify the features of the subject matter and the limits of proof in a criminal case of cybercrimes of this type. Still others need to use the methodology for investigating such cybercrimes in a cyclical mode with feedback loops to identify each of the crimes committed in the aggregate and differentiate their elements. The formation of hierarchical systems of legal algorithms of various types and purposes makes it possible to create on their basis a number of problem-oriented computer programs that ensure the proper enforcement of interactive information systems for the processing of electronic documents and other information in the identification, disclosure and investigation of crimes in the field of digital economy and finance.

Keywords

cybercrimes; digital economy and finance; digital rights; digital financial assets; market manipulation; legal algorithms; interactive information systems.

For citation: Rastoropov S.V., Prorvich V.A. (2024) Information Bases of Modern Criminal Law Protecting Subjects of Digital Economy and Finance. *Law. Journal of the Higher School of Economics,* vol. 17, no. 2, pp. 143–169 (in Russ.) DOI:10.17323/2072-8166.2024.2.143.169

Введение

Обсуждение проблем создания надежной системы уголовно-правовой защиты современных общественных отношений в условиях перехода к информационному обществу и экономике знаний неизбежно приводит к выводам о необходимости формирования ее прочного научно обоснованного фундамента. Исследования показывают, что он должен иметь интегрированный характер, не только объединяя возможности юридических наук и наук информационного блока, но и фокусируя усилия ученых и специалистов на формализацию новых проблем борьбы с современным криминалом. Это позволит создать современный высокотехнологичный инструментарий выявления, пресечения и профилактики преступлений рассматриваемого вида, выверенный с правовой точки зрения.

Вектор научных исследований и разработок в данной сфере задан в основополагающих указах Президента России[1]. Их правовые установки носят стратегический характер, определяя важнейшие задачи, которые предстоит решить деятелям всех юридических наук и специалистам-практикам. При этом речь идет не только о создании новой системы регулирования правоотношений субъектов будущего информационного общества различного вида и уровня, но и об их надлежащей уголовно-правовой защите.

Особенно трудные проблемы, связанные с постановкой и выполнением соответствующих исследований, возникают, когда новые проблемы борьбы с киберпреступностью наслаиваются на ставшие привычными способы их решения. Дополнительные трудности связаны с тем, что криминал не ограничен какими-либо рамками в разработке и реализации преступных схем, включая использование самых современных информационных технологий. Правоохранительные же органы при этом обязаны действовать строго в рамках правовых предписаний.

Соответственно, при разработке методик выявления, раскрытия, расследования и профилактики новых, «высокотехнологичных» видов преступлений в сфере цифровой экономики и финансов, возникает необходимость не только комплексного, но и взаимосвязанного, взаимообусловленного развития всех наук уголовно-правового блока. Однако анализ публикаций, раскрывающих соответствующие проблемы и способы их решения, показывает, что возможности синхронизации их развития в интересах уголовно-правовой защиты субъектов информационного общества и экономики знаний далеко не однородны.

Целью настоящей работы является поиск основных подходов к формированию единого, интегрированного фундамента, объединяющего возможности инструментария, созданного в рамках наук уголовно-правового и информационного блоков, для создания в конечном итоге проблемно-ориентированного программного обеспечения, сориентированного на применение интерактивных информационных систем, необходимых для надлежащей обработки электронных документов и иной электронной информации о киберпреступлениях в сфере традиционной и цифровой экономики и финансов.

[1] Стратегия развития информационного общества Российской Федерации на 2017-2030 годы, утвержденная Указом Президента РФ от 09.05. 2017 № 203; Указ Президента РФ «О национальных целях и стратегических задачах развития Российской Федерации до 2024 года» от 07.05. 2018 № 204; Национальная программа «Цифровая экономика Российской Федерации». Утверждена президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24.12.2018 № 16; Указ Президента РФ «О развитии искусственного интеллекта в Российской Федерации» от 10.10. 2019 № 490 // СПС КонсультантПлюс.

Для ее достижения рассмотрены основные подходы к формализации важнейших проблем на стыке юридических наук и информатики, решение которых позволяет сформировать информационные модели киберпреступлений в сфере цифровой экономики и финансов и разработать на их основе юридические алгоритмы обработки электронных документов и иной электронной информации для оперативного выявления в них признаков киберпреступлений, их своевременного раскрытия и надлежащего расследования.

1. Роль информатики в криминологических исследованиях киберпреступности в сфере цифровой экономики и финансов

Наибольший объем исследований надлежащей криминализации части формирующихся общественных процессов при переходе к информационному обществу и экономике знаний находится в сфере компетенции криминологии. Один из ведущих ученых-криминологов — В.В. Лунеев определил криминологию как «относительно самостоятельную, комплексную социально-правовую науку об изучении закономерностей и тенденций преступности, ее причин и условий, личности преступника и его преступного поведения, об изыскании адекватных методов их исследования и прогнозирования в целях разработки эффективных направлений социально-правового контроля преступных проявлений, их предупреждения и минимизации». При этом он оговаривал, что криминология является одним из направлений более общих наук о выживании и безопасности в общественно опасной среде[2] [Лунеев В.В., 2010: 27].

Отталкиваясь от данного положения, допустимо сделать выводы о том, что характер опасности общественной среды существенно изменился и продолжает быстро изменяться. Формируются новые критерии не только выживания, но и дальнейшего развития нашего государства и общества. При этом важно принимать во внимание особую опасность не только ряда внутренних факторов общественного развития, связанных с образованием новых видов зависимости большинства граждан от смартфонов, переключения личного общения на контакты в социальных сетях, но и других, внешних факторов,

В последние годы резко возрос поток дезинформации, фальшивых новостей и экстремистских материалов из внешних источников, осо-

[2] Лунеев В. В. Криминология / Большая Российская Энциклопедия. Т. 16. М., 2010. С. 27.

бенно после начала специальной военной операции. Негативное влияние на российскую экономику, финансовую систему и общественное развитие в целом оказывают и тысячи различных санкций, принятых руководством западных стран. Неблагоприятное сочетание перечисленных и множества иных внутренних и внешних факторов требует системы контрмер, среди которых важную роль призваны сыграть и науки уголовно-правового блока.

При их разработке важно учитывать, что в современной криминологии [Максимов С.В., 2018: 476] выделена ее Общая часть, раскрывающая важнейшие понятия, методы исследования преступности, начиная от ее причин и заканчивая прогнозированием как преступности в целом, так и индивидуального преступного поведения отдельных субъектов, и Особенная часть, раскрывающая особенности различных видов преступности, включая ее новые виды. В то же время изучение закономерностей и тенденций развития преступности «должно опираться на математику, юридическую и иную социально-экономическую статистику, теорию вероятностей и закон больших чисел значительного ряда показателей, что дает возможность перейти от случайного и единичного к устойчивому и массовому, и уже на этой основе вырабатывать адекватные меры борьбы с преступностью и ее предупреждения»[3] .

Правда, перечисляя различные виды преступности, он не отметил ее принципиально новых видов [Лапин В.О., 2022: 7], основанных на широком применении компьютеризованных устройств и самых современных информационных технологий [Абдулвалиев А.Ф., 2021: 10–44]. Но за 15 лет, прошедших с момента подготовки указанной публикации, количество таких преступлений увеличилось почти в 50 раз, а их доля возросла до 1/3 всех зарегистрированных преступлений. К тому же отмечается высочайший уровень латентности не только отдельных видов подобных преступлений в финансовой сфере [Опальский А.П., 2022: 3–10], но и киберпреступности в целом.

Во многом это объясняется тем, что существенная часть общественных отношений в настоящее время уже перешла в виртуальное информационное пространство компьютерных сетей, организованное по законам прикладной математики, кибернетики и информатики [Романовский М.Ю., 2020: 9–10]. При этом часть ученых и специалистов, непосредственно участвующая в создании научных основ формирования данного искусственно созданного пространства, его управления и развития, широко использует искусственные алгоритмические языки. Из отмеченных многими учеными теснейших связей языка и мышления че-

[3] Там же. С. 28.

ловека неизбежно следует ряд констатаций специфики принципиально новых общественных отношений и связанных с ними ментальных явлений, в том числе криминального характера.

Прежде всего обращают на себя внимание общественные процессы, связанные со всеобщей «цифровизацией», изменяющей условия жизни каждого гражданина страны. В рамках данных процессов происходит все более активное использование информационных технологий в промышленности, государственном управлении, образовании, здравоохранении и практически во всех других сферах жизни. Развиваются самые современные сферы телекоммуникаций, позволяющие создавать уже не только «умные дома», но и «умные города».

Соответственно, и преступность, связанная с данными новыми и весьма своеобразными сферами общественных отношений, приобретает качественно новый характер [Жданов Ю.Н., 2020: 16–18]. Вполне естественно, что многие стереотипы, ставшие давно привычными в сфере уголовно-правовых наук, не позволяют успешно применять возможности, имеющиеся в сфере прикладной математики, кибернетики и информатики, а также других естественных наук, для борьбы с киберпреступностью. Для преодоления данных стереотипов юристам необходимы естественнонаучные знания и профессиональные компетенции, на что внимание высшего руководства страны обратили ведущие ученые во время недавнего празднования 300-летнего юбилея Российской Академии наук.

2. Использование инструментария наук информационного блока в уголовном судопроизводстве по киберпреступлениям

2.1. Парадоксы, связанные с применением понятия «цифра» в условиях перехода к информационному обществу

Характерной особенностью современного этапа развития информационного общества является создание крупных программно-аппаратных комплексов различного назначения, получивших названия «платформ», сориентированных на решение задач государственного, отраслевого и иного уровней, вплоть до оказания широкого спектра услуг каждому российскому гражданину [Савенко Н.Е., 2023: 145]. Происходит разработка и внедрение сложнейших комплексов системного и прикладного программного обеспечения, для создания и внедрения которого уже создана новая государственная инфраструктура, нацеленная на системное применение информационных технологий во всех сферах

жизни и деятельности российского общества. Не должна остаться в стороне и сфера борьбы с киберпреступностью.

Основы кибернетики, позволяющей с помощью математических методов управлять потоками самой разнообразной информации, а затем и принципы, на которых должны создаваться современные компьютеры, позволяющие реализовать практически данные методы, были разработаны группой ученых и специалистов, возглавляемой Н. Винером и Дж. фон Нейманом. Компьютеры с фон-Неймановской архитектурой оказались востребованными не только 75 лет назад, но и в настоящее время[4]. Кроме взаимосвязанных электронных блоков — процессора, устройств памяти, ввода и вывода информации и некоторых других — их неотъемлемой частью стали компьютерные программы, как системные, управляющие функционированием каждого из его блоков и компьютером в целом, так и прикладные, предназначенные для выполнения задач пользователя. При этом изначально было специально оговорено, что программное обеспечение компьютера может изменяться и дополняться в процессе его использования.

В качестве одного из принципов работы компьютеров фон-Неймановской архитектуры стало использование двоичного кода для любой информации, создаваемой, обрабатываемой и хранящейся в памяти таких компьютеров. Но содержательные особенности создаваемой, преобразуемой и используемой информации формируется потоками чисел, а цифры 0 и 1 используются лишь для кодирования числовой информации, ввиду особенностей функционирования миллиардов электронных ячеек, используемых в этих компьютерах.

Таким образом, широко используемые понятия, связанные с процессами всеобщей цифровизации нашего общества — «цифровые технологии», «цифровые платформы», «цифровая экономика», «цифровые права»[5] и т.п., означают создание весьма сложных комплексов информационных технологий, управляющих разнообразными информационными системами с использованием системного и прикладного программного обеспечения.

Но цифр всего 10, от 0 до 9, а в двоичном коде их две — 0 и 1, и они используются для записи любых чисел, не только целых, во много миллионов и миллиардов, но и дробных, в ноль целых и пять сотых процента, рациональных, иррациональных и даже мнимых. Таким образом, цифры и их комбинации — лишь узаконенный правилами математики

[4] Журавлев Ю.И. Кибернетика / Большая Российская Энциклопедия. Т. 13. М., 2009. С. 629–630.

[5] Федеральный закон № 34-ФЗ от 18.03.2019 // СПС КонсультантПлюс.

способ кодирования чисел, несущих информацию о количественных характеристиках любого процесса или явления, включая сведения о киберпреступлениях.

В то же время распространившаяся в последнее время среди специалистов юридических наук уголовно-правового блока привычка отождествлять числа с цифрами создает высокий уровень рисков юридических ошибок. В частности, при проведении любых экономических и иных расчетов происходит накопление погрешностей, особенно при использовании дробных чисел. В неудачных математических моделях, используемых судебными экспертами, погрешности расчетов по величине могут быть вполне сопоставимыми с результатами расчетов. Следователи, прокуроры и судьи, не обладающие необходимым для обязательной проверки и оценки соответствующих доказательств профессиональными компетенциями, оказываются не в состоянии выявить математические ошибки, которые становятся юридическими, изменяющими судьбы людей [Романовский М.Ю., 2020: 9–10].

Это еще раз подтверждает правильность и своевременность предложений, сделанных ведущими учеными страны, о необходимости срочного введения курса математики и других естественных наук в программы подготовки и профессиональной переподготовки юристов.

2.2. Тенденции развития процессов цифровизации в сфере наук уголовно-правового блока

Весьма упрощенные понятия многих юристов о происходящих в обществе процессах цифровизации приводят не только к ряду проблем в правоприменении. Не менее важно обратить внимание и на процессы развития наук уголовно-правового блока, в том числе связанные с имплементацией в них инструментария, развитого в рамках наук информационного блока. Среди них необходимо выделить следующие группы проблем.

Прежде всего это проблемы технократического характера, проявляющихся в предложениях многих ученых не только о применении «цифровых» следов преступлений в качестве доказательств при расследовании соответствующих уголовных дел, но и о введении криминологического и уголовно-правового понятия «цифровые преступления».

Опросы показывают, что некоторые наши коллеги не задумываются над тем, что при нажатии на клавишу компьютера, к примеру, с буквой «а», направляют в память число 224, преобразованное с помощью определенной программы в группу электронных импульсов двух видов, последовательность которых определяется следующим чередованием условных нулей и единиц в двоично-восьмеричном коде: 11100000. При

нажиме клавиши с буквой «А» программа отправляет в память число 192 в виде другой последовательности электронных импульсов в двоично-восьмеричном коде: 11000000.

Соответствующие преобразования символов обычного «человеческого» языка — как с использованием латиницы, так и кириллицы на «компьютерный» язык осуществляется программным путем с помощью специально созданной универсальной системы кодов ASCII. Эти сигналы передаются между микросхемами компьютера и их элементами со скоростью в миллиарды импульсов в секунду, не оставляя в большинстве из них никаких следов.

Более того, даже при формировании потоков экономических данных числа, представленные в десятичной системе, не преобразуются в двоичную систему, а кодируются в системе компьютерных кодов ASCII. Цифра «0» в десятичной системе отнюдь не эквивалентна цифре «0» в двоичной системе, а кодируется числом 48 или двоично-восьмеричным числом 00110000. Цифра «1» в десятичной системе не соответствует цифре «1» в двоичной системе, а кодируется числом 49 или двоично-восьмеричным числом 00110001.

Даже из этих простейших примеров очевидно, что следы киберпреступлений в сфере цифровой экономики и финансов носят закодированный информационный характер. Для их выявления необходима разработка проблемно-ориентированных информационных моделей и алгоритмов, на основе которых возможно создание соответствующих компьютерных программ. В свою очередь, формирование доказательств по уголовному делу предполагает применение программного обеспечения в составе интерактивных информационных систем, позволяющих выполнять процедуры обработки информации, имеющей правовой статус, в диалоговом режиме.

Кроме того, в правоприменительной практике следователи, оперативные сотрудники, эксперты и специалисты активно используют самые разнообразные компьютерные программы, как отечественные, так и иностранные. В материалах уголовных дел даются ссылки на названия этих программ, а также на названия интернет-ресурсов, к которым применялись данные программы, в том числе с их адресами. Но во многих случаях оказывается, что описание моделей и алгоритмов, на основе которых были созданы эти программы, правоприменителям неизвестны. Фактически подобные доказательства оказываются полученными с помощью «черного ящика», а их надлежащая проверка и оценка в соответствии с установленными ст. 17, 87 и 88 Уголовно-процессуального кодекса Российской Федерации (далее–УПК РФ; УПК) требованиями становится невозможной.

Стремление наших коллег к широкому использованию современных информационных технологий и компьютерных программ различного вида вполне понятно. Однако из-за преобладания технократических подходов, имеющих весьма отдаленное отношение к наукам уголовно-правового блока, возникает высокий уровень рисков совершения юридических ошибок. О создании в рамках данных подходов системы уголовно-правовой защиты субъектов информационного общества говорить в принципе не приходится [Шмонин А.В., 2017: 73].

Таким образом, формирование системы уголовно-правовой защиты субъектов цифровой экономики и финансов происходит в условиях «несимметричной» стыковки инструментария, развитого в науках уголовно-правового и информационного блоков. С одной стороны, детально разработанная в сфере уголовно-правовых наук система правоприменения дополняется недостаточно глубокими знаниями некоторых ученых-юристов о современной математике, кибернетике и информатике. С другой стороны, детально разработанная в науках информационного блока система обработки информации различного характера дополняется их весьма поверхностными знаниями об особенностях уголовного права, уголовного процесса, криминалистики, судебной экспертизы и оперативно-розыскной деятельности.

Для кардинального изменения ситуации необходима научная обоснованность подходов к надлежащей имплементации инструментария, созданного в рамках наук информационного блока, в систему наук уголовно-правового блока. При разработке соответствующих информационных моделей важно понимать особенности киберпреступности в сфере цифровой экономики и финансов. В свою очередь, на основе юридических алгоритмов процессуально регламентированных действий по обработке документированной информации, имеющей значение для расследуемого уголовного дела, могут быть не только созданы необходимые компьютерные программы, но и их подробное описание на языке, доступном всем участникам уголовного судопроизводства.

3. Особенности новых видов киберпреступности в системе цифровых прав и цифровых финансовых активов

В связи с обозначенными выше основными особенностями всеобщей цифровизации российского государства и общества необходимо подчеркнуть ряд важных особенностей введенного законодателем уже почти пять лет назад принципиально нового понятия цифровых прав. Оно было связано отнюдь не только с использованием самых разнообразных

информационных систем, включающих различные базы данных, системы управления базами данных с соответствующими программными средствами и иную информацию. Одновременно было указано на введение и нового правового понятия — «правил информационной системы», причем «установленных ее обладателем».

Цифровые права были отнесены законодателем к новой разновидности обязательственных прав, причем обязательства и права требования их субъектов формируются не только в рамках договора, оформленного надлежащим образом. Во многих случаях они могут возникать путем признания пользователем информационной системы ее правил «по умолчанию», т.е. «присоединения» к ним даже без ознакомления с их содержательными особенностями. При этом требования об обязательном соответствии таких правил нормам законодательства, а также о том, кто и в каком порядке осуществляет соответствующий контроль, в явном виде сформулированы не были.

Аналогичные правовые новеллы были использованы при введении понятия «цифровых финансовых активов»[6], под которыми понимаются цифровые права, выпуск, учет и обращение которых возможны только путем внесения записей в информационной системе на основе распределенного реестра. Таким образом, законодатель сделал следующий шаг в дальнейшей детализации содержательных особенностей понятия цифровых прав как новой разновидности обязательственных прав. 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. При этом ни о каких цифрах речи нет.

Однако здесь было введено существенное дополнение характеристики данного правового понятия. Совершение перечисленных выше сделок с объектами российских цифровых прав допускается и по правилам иностранных информационных систем. Эту правовую новеллу можно было бы приветствовать в случае принятия международным сообществом универсальной системы правовой регламентации правил информационных систем, создаваемых их обладателями в любом государстве. Соответственно для разрешения гражданско-правовых споров в системе цифровых прав мог быть создан международный арбитраж с соответствующими правилами и процедурами, признанными всеми государствами–членами ООН [Жданов Ю.Н., 2020: 16–18]. Но пока такая система не создана, а опережение естественного развития глобальных событий в правовой сфере

[6] Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ // СПС КонсультантПлюс.

финансово-экономических отношений, если оно признано необходимым, должно быть надлежащим образом подготовленным.

Подобная ситуация сложилась и при введении цифрового рубля[7]. С одной стороны, законодателем были подробно описаны процедуры выполнения расчетов в цифровых рублях в рамках платформы цифрового рубля Банка России. Фактически цифровой рубль был определен как цифровой финансовый актив, выполняющий функцию электронного средства платежа. При этом создание электронного кошелька на платформе ЦБ РФ, его наполнение цифровыми рублями и операции с ними предусмотрены не только через интернет-приложение любого российского банка, подключенного к платформе Банка России, но и иностранного. Получая доступ к своему электронному кошельку через интернет-приложения нескольких банков, как отечественных, так и иностранных, его обладатель фактически получает возможность оперировать цифровыми рублями с территории иностранного государства.

Понятно, что это открывает новые возможности для субъектов цифровых прав по осуществлению взаиморасчетов в национальных валютах. С другой стороны, при этом вводится ряд правовых новелл на уровне нормативных правовых актов Банка России. Как будут разрешаться гражданско-правовые споры с обладателями российских цифровых рублей, которыми они оперировали с территории иностранных государства в рамках связи соответствующих российских и иностранных информационных систем, пока не определено.

Нельзя забывать об принятых два года назад западными странами санкциях, в результате которых были заморожены валютные резервы Банка России в размере около 300 млрд. долл. По различным оценкам, еще более крупные по размеру валютные средства западные банки заморозили у российских фирм и частных лиц. Более того, в настоящее время активно обсуждаются новые меры, нацеленные на конфискацию этих замороженных средств в их информационных системах, в том числе путем существенного изменения их правил.

С точки зрения рассматриваемых в настоящей статье проблем формирования надлежащей уголовно-правовой защиты субъектов цифровой экономики и финансов следует сделать ряд акцентов на особенностях нестыковок правил информационных систем, образующих цепочку, которую приходится использовать субъекту цифровых прав. Кроме этого, важно обратить внимание и на особенности оригинального программного обеспечения, которое используется обладателями информационных систем. Необходимо учитывать и возможные несты-

[7] Федеральный закон от 24.07.2023 № 340-ФЗ // СПС КонсультантПлюс.

ковки сочетания используемого программного обеспечения и правил информационных систем на уровне их обладателей, а также нарушения действующего законодательства.

Изучение новых проблем уголовно-правового характера показывает, что исследование особенностей системы обязательственных прав нового вида должны фокусироваться не только на их соответствии требованиям действующего гражданского, финансового, информационного и иного специального законодательства. Необходима разработка научно обоснованных критериев для контроля за особенностями совокупностей правил тех информационных систем, которые используются при совершении киберпреступлений различного вида.

Первоочередное значение приобретают выверенные в правовом плане информационные технологии для «выстраивания» алгоритмов конкретных процедур преобразования электронной информации субъектов цифровых прав в цепочке использованных ими информационных систем. Это позволяет установить, в какой именно информационной системе произошло нарушение цифровых прав их субъекта, ставшего потерпевшим, а затем выявить особенности ее правил, а также роль обладателя данной информационной системы в возможном нарушении обязательственных прав потерпевшего.

Анализ особенностей правовых и информационно-технологических особенностей формирования юридических алгоритмов, характеризующих систему транзакций субъектов цифровых прав через определенные совокупности информационных систем показывает, что среди них можно выделить несколько групп, имеющих существенные различия.

К первой группе можно отнести систему алгоритмов, позволяющих сформировать развернутую уголовно-правовую характеристику преступлений данного вида. Ко второй — алгоритмы формирования предмета доказывания по соответствующим уголовным делам, а также установления пределов доказывания. К третьей — алгоритмы формирования криминалистических методик расследования преступлений в сфере цифровых прав на основе их криминалистической характеристики. К четвертой — алгоритмы обработки электронных документов и иной информации в рамках оперативно-розыскных мероприятий, позволяющих выявить признаки совершения преступлений данного вида. К пятой — алгоритмы информационно-методического обеспечения применения специальных знаний судебных экспертов и специалистов при расследовании уголовных дел о преступлениях данного вида.

Следует обратить внимание на то, что элементы каждой из перечисленных групп алгоритмов, а также система связей между ними имеют ряд существенных отличий. В то же время исследования показывают, что при их дальнейшей разработке могут быть использованы единые

подходы на основе важнейших принципов наук уголовно-правового блока. На основе иерархически выстроенной системы данных алгоритмов может быть создан пакет соответствующих компьютерных программ, обеспечивающих проблемно-ориентированную обработку электронной и иной информации в рамках соответствующих интерактивных информационных систем. При этом возникают новые возможности для контроля за сохранением правового статуса промежуточных и итоговых результатов обработки электронных документов и иной информации, имеющей значение для уголовного дела.

4. Формирование нового инструментария в системе наук уголовно-правового блока с учетом особенностей киберпреступности в сфере цифровой экономики и финансов

4.1. Особенности разработки и применения юридических алгоритмов выявления, раскрытия и расследования киберпреступлений

Одной из актуальных проблем уголовно-правовой защиты субъектов цифровой экономики является все более широкое применение в системе обязательственных прав, в том числе для заключения «умных» или «смарт-» контрактов, технологии «блокчейн» [Тимошенко А.А., 2023: 21–23]. С ее использованием созданы также сотни различных видов и разновидностей криптовалют, а также система различных «криптобирж», в рамках которых производится обмен «криптовалют» на валюты соответствующих государств [Янковский Р.М., 2020: 43]. При этом законодательством России подобные биржи не предусмотрены, но владение, пользование и распоряжение криптовалютами не криминализовано. Однако они нередко используются при совершении преступлений различных видов, преимущественно связанных с дачей и получением взяток, оплатой наркотиков, исполнителей терактов и т.п.

Кроме перечисленных выше имеется и ряд иных пробелов и противоречий в сложившейся к настоящему времени системе уголовно-правовой защиты субъектов цифровой экономики и финансов — как на уровне правотворчества, так и на уровне правоприменения. Достаточно упомянуть о дискуссиях о самом понятии «киберпреступления», что не позволяет создать научно обоснованную и выверенную с правовой точки зрения классификацию таких преступлений.

Главной особенностью подобных преступлений является проникновение криминала в те сферы жизни общества, где формируются, передаются,

изменяются и используются интенсивные потоки самой разнообразной информации. Напомним, что в одной из отраслей науки кибернетики — лингвистической кибернетики — были развиты средства общения человека с компьютером, в том числе на «естественном» языке, а также структурные модели обработки, анализа и оценивания информации.

В такой ситуации постановка и реализация криминологических исследований киберпреступности приобретает особенно большое значение. Ряд общих установок о широчайших возможностях, которые дают современной криминологии математика, кибернетика, информатика и другие науки, нуждается в конкретизации на базе осмысления важнейших тенденций развития информационного общества и особенностей новых криминальных проявлений.

Актуальность постановки соответствующих исследований и разработок существенно возрастает и из-за быстрого нарастания трудноразрешимых проблем правоприменения в данной сфере. Анализ содержательных особенностей уголовно-правовых норм по преступлениям в сфере экономики показывает, что среди них к рассматриваемым проблемам защиты субъектов цифровой экономики и финансов можно отнести лишь очень немногие, причем введенные в действие задолго до принятия законодательства о цифровых правах, цифровых финансовых активах, цифровом рубле и других правовых понятиях «цифрового» характера. К ним с долей условности можно отнести следующие.

Прежде всего это диспозиция ст. 158 Уголовного кодекса Российской Федерации (далее — УК РФ; УК), в п. г ч. 3 которой использовано понятие «электронные денежные средства», ст. 159^3 УК «Мошенничество с использованием электронных средств платежа», в которой также использовано данное «электронное» понятие. В ст. 159^6 УК «Мошенничество в сфере компьютерной информации» указывается также на средства хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационные сети.

Понятия «Интернет», «информационно-телекоммуникационные сети», «интерактивные ставки» использованы законодателем в диспозиции ст. 171^2 УК «Незаконные организация и проведение азартных игр». Такая имплементация понятий из сферы наук информационного блока в уголовное право, с одной стороны, оправдана, поскольку позволяет в рамках правоприменения использовать сложившуюся систему понятий в данной сфере общественных отношений. С другой стороны, встают вопросы о раскрытии уголовно-правового смысла данных понятий. Это особенно важно, когда законодатель использует некоторые из них для раскрытия содержания других новых понятий, используя метод исключения. Ряд подобных понятий — «электронные средства массовой

информации», «Интернет», «информационно-телекоммуникационные сети» — использован законодателем и в диспозиции ст. 185[3] УК «Манипулирование рынком».

В ст. 187 УК «Неправомерный оборот средств платежей», кроме перечисленных выше, использованы также понятия «электронные средства», «электронные носители информации», «технические устройства», «компьютерные программы», предназначенные для неправомерного осуществления приема, выдачи, перевода денежных средств.

Таким образом, в ряде уголовно-правовых норм по преступлениям в сфере экономики использованы понятия, относящиеся к сфере информатики, в том числе в сочетании с экономическими и уголовно-правовыми понятиями. В ряде других уголовно-правовых норм по преступлениям рассматриваемого вида некоторые из подобных понятий использованы в «неявном виде». Речь идет о статьях, в которых указано о действиях граждан, связанных с получением денежных сумм, либо осуществлением платежей различного вида и назначения, поскольку они осуществляются через информационные системы российских и иностранных банков. Но «цифровых» понятий законодатель и в них не использовал.

Многие уголовно-правовые нормы в той или иной мере связаны с различными реестрами, предназначенными для государственной регистрации определенных видов прав и объектов движимого и недвижимого имущества, которые фактически являются информационными системами с проблемно-ориентированными базами данных и системами управления ими.

В рамках юридических алгоритмов, сформированных для раскрытия бланкетных, отсылочных и смешанных диспозиций уголовно-правовых норм по преступлениям в сфере цифровых прав, назрела необходимость использования не только уголовного, гражданского и специального законодательства, но и результаты анализа правил, использованных преступниками информационных систем. При этом в подобных правилах, созданных обладателями данных информационных систем, могут быть использованы самые разнообразные узкопрофессиональные термины, требующие раскрытия с применением знаний судебных экспертов и других специалистов в данной сфере.

4.2. Особенности информационных моделей киберпреступлений в сфере цифровой экономики и финансов

Перечисленные выше уголовно-правовые понятия в той или иной степени связаны с понятием «компьютер», преимущественно, в качестве

способа совершения киберпреступлений в сфере экономики. Нередко при этом выявляются «сопутствующие» преступления, образующие с «основным» совокупность. Их субъектами могут использоваться различные формы соучастия в таких преступлениях, например, при финансировании экстремистской и террористической деятельности [Бычков В.В., 2022: 166].

Обращение к уголовно-правовым нормам Главы 28 УК «Преступления в сфере компьютерной информации» показывает, что в четырех ее статьях (ст. 272–274[1]) использованы следующие понятия: «компьютерная информация», «охраняемая законом компьютерная информация», а также такие уголовно наказуемые деяния, как «блокирование, модификация либо копирование компьютерной информации». Кроме того, дано определение: «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи». Здесь также какие-либо цифровые понятия законодателем не использованы.

Более того, введено такое понятие, как «вредоносная компьютерная программа», которое было связано с предыдущим понятием «компьютерная информация». Раскрывая особенности данного понятия, законодатель указал, что «вредоносность» данных программ связана с тем, что они «заведомо предназначены для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации». Кроме этого, введено уголовно-правовое понятие «нейтрализация средств защиты компьютерной информации». Законодатель вводит ряд новых понятий, связанных с криминальным нарушением «правил эксплуатации» не только средств хранения, обработки или передачи компьютерной информации, но и «информационно-телекоммуникационных сетей». Это также «оконечное оборудование» и «правила доступа» к информационно-телекоммуникационным сетям.

Новизной с точки зрения российского уголовного права отличаются и понятия «критическая информационная инфраструктура Российской Федерации», а также «неправомерное воздействие» на нее. Эти понятия дополнены понятиями «охраняемая компьютерная информация, содержащаяся в критической информационной инфраструктуре Российской Федерации», «правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации», «информационные системы», «автоматизированные системы управления», «сети электросвязи», относящихся к критической информационной инфраструктуре Российской Федерации, «правила доступа к информации, информационным системам, информационно-телеком-

муникационным сетям, автоматизированным системам управления, сетям электросвязи».

С использованием данных понятий открывается ряд возможностей не только для выявления определенных видов совокупностей преступлений в сферах экономики и компьютерной информации, но и при раскрытии особенностей бланкетных, отсылочных и смешанных диспозиций уголовно-правовых норм по преступлениям в сфере экономики [Бычков В.В., 2022: 166]. Применение для этого различных положений уголовного, гражданского и специального законодательства требует разработки специальных средств контроля, чтобы не допустить выхода сформированной таким образом развернутой уголовно-правовой характеристики за рамки уголовного права и не допустить юридических ошибок.

Несколько иной точки зрения придерживался Л.Д. Гаухман, предлагая использовать для раскрытия бланкетных диспозиций только уголовно-правовые нормы. Что касается положений гражданского и специального законодательства, то он предлагал подготовить закрытый перечень таких положений и использовать его в качестве официального приложения к Уголовному кодексу [Гаухман Л.Д., 2013: 111–116].

Однозначного решения данной проблемы до сих пор не найдено, поэтому вероятность юридических ошибок следователей при формировании развернутых уголовно-правовых характеристик преступлений в сфере цифровой экономики остается весьма высокой. Ввиду необходимости использования при раскрытии бланкетных диспозиций по преступлениям в сфере цифровой экономики правовых актов нового вида — правил информационных систем, созданных их обладателями, в том числе иностранными, — эти риски нередко вырастают до недопустимых уровней.

Исследования с применением инструментария не только уголовно-правового, но и информационного блока показали, что при формировании некоторых уголовно-правовых норм о финансовых преступлениях в сфере цифровых прав, связанных с цифровыми финансовыми активами, эмиссионными ценными бумагами, выпускаемыми только в виде электронных документов и обращаемыми только с использованием определенной совокупности информационных систем профессиональных участников фондового рынка, законодатель уже начал использовать математические модели вероятностного характера. При раскрытии их бланкетных диспозиций встает ряд проблем с идентификацией признаков объекта и предмета преступления, а также его объективной стороны.

С точки зрения математики процесс правотворчества имеет сходство с функцией многих переменных либо формированием интегрального

преобразования[8]. В результате такой «юридической свертки» многочисленных положений законодательства, имеющих отношение к определенному виду преступления в сфере цифровой экономики, получается лаконичная формулировка бланкетной, отсылочной или смешанной диспозиции соответствующей уголовно-правовой нормы.

Попытка юриста-правоприменителя раскрыть такую диспозицию и сформировать развернутую уголовно-правовую характеристику конкретного преступления в рамках правового поля, в котором, по мнению правотворцев, действуют законопослушные субъекты цифровых прав, представляет собой «обратную юридическую задачу». Решение таких задач оказывается намного сложнее, чем решение «прямых» задач криминологами, и очень часто приводит к неточным и ошибочным результатам.

Более детальный анализ особенностей подобной «юридической свертки», характеризующей преступные проявления в системе цифровых прав, приводит к аналогиям с формированием интегральных уравнений различного рода[9]. Из-за ряда неопределенностей в левой и правой частях «юридического интегрального уравнения», оно имеет бесконечное множество решений, что приводит к высокому уровню рисков совершения юридических ошибок при попытках адаптировать уголовно-правовые нормы к системе цифровых прав.

Результаты исследований, нацеленных на конкретизацию содержательных особенностей данных проблем и нахождение путей их скорейшего решения, показали, что с помощью нынешнего инструментария в системе юридических наук уголовно-правового блока в ближайшее время это вряд ли возможно. На научных конференциях по компьютерной и информационной безопасности, проводившихся в последние годы, большинство докладов было посвящено различным аспектам применения именно технических и программных средств. Проблемы уголовно-правового обеспечения защиты прав и законных интересов субъектов цифровых прав различного вида и уровня практически не затрагивались.

Ситуация носит не только субъективный, но и объективный характер. В первую очередь речь идет о разработке новых подходов к криминализации таких общественных процессов, которые развиваются в искусственно созданном информационном пространстве компьютерных сетей, но проявляются в материальном мире, нанося существенный ущерб гражданам, организациям, государству и обществу в целом.

---

[8] Брычков Ю. А. Интегральное преобразование / Большая Российская Энциклопедия. Т. 11. М., 2008. С. 425–426.

[9] Хведелидзе Б. В. Интегральное уравнение. Там же. С. 426–427.

Изучение взаимопроникновения общественных отношений в искусственно созданном информационном пространстве и материальном мире показывает, что важную роль в их формализации для создания надлежащей уголовно-правовой защиты субъектов цифровых прав может сыграть разработка соответствующих информационно-математических моделей. В качестве одного из критериев их адекватности могут использоваться результаты сопоставления математических расчетов с реалиями правоприменительной практики.

4.3. Особенности разработки информационных моделей и методов компьютерного моделирования преступной деятельности в сфере цифровой экономики и финансов

Форсирование криминологических исследований новых видов преступных проявлений приходится осуществлять в многофакторных условиях перехода к информационному обществу и экономике знаний. В качестве одного из направлений методического обеспечения, нацеленного на их выявление, формализацию и надлежащую криминализацию, может быть использовано компьютерное моделирование [Лузгин И.М., 1981: 7]. В его основе заложен ряд математических моделей, позволяющих дополнить процесс криминологических исследований в сфере цифровой экономики и финансов прямым математическим моделированием деятельности законопослушных субъектов цифровых прав, а также результатами математического моделирования преступлений данного вида, по которым вынесены приговоры суда. Такое моделирование может проводиться в рамках нескольких взаимосвязанных и взаимодополняющих этапов. При этом на каждом из них первостепенное внимание должно обращаться на полное соблюдение требований используемых положений законодательства, в том числе с учетом их взаимных связей.

На первом этапе производится формализация характеристик правового поля, в рамках которого и проявляются особенности взаимодействия законопослушных субъектов цифровых прав. При этом выделяются особенности прав и обязанностей как обладателей информационных систем, так и потребителей оказываемых ими услуг. Поскольку речь идет об использовании для такого моделирования определенных совокупностей положений действующего гражданского и специального законодательства, то при выявлении правовых пробелов они могут быть заполнены по результатам анализа обычаев делового оборота, сложившихся в данной сфере.

В результате выполнения данного этапа создается возможность формирования системы «информационных эталонов», характеризующих

деятельность законопослушных субъектов в сферах цифровой экономики. При возникновении неопределенностей в некоторых из информационных эталонов или нескольких их вариантов из-за нестыковок положений различных видов законодательства (прежде всего на уровне подзаконных нормативных актов) они могут устраняться различными способами, в том числе с использованием эмпирических данных.

Предварительные оценки показывают, что количество подобных информационных эталонов может измеряться десятками тысяч. Для упрощения их применения на следующих этапах моделирования преступных проявлений в сфере цифровой экономики на первом этапе моделирования может быть сформировано несколько тематических слоев соответствующего правового поля. При использовании подобного «многослойного» моделирования появляются новые возможностей для снижения отмеченных неопределенностей путем «межслойного оверлея» — сопоставления особенностей различных групп информационных эталонов с подобными характеристиками субъектно-субъектных и субъектно-объектных отношений в сфере цифровых прав.

На втором этапе компьютерного моделирования могут быть сформированы специальные слои информационных эталонов другого типа. Они призваны создавать ориентиры надлежащего формирования правил, которые устанавливаются обладателями информационных систем различного вида в полном соответствии с требованиями законодательства. Это создает возможности после выявления отклонения правил какой-либо информационной системы от эталонов данного слоя выполнить их развернутое сопоставление с положениями законодательства, регламентирующими данные виды деятельности, отраженными в соответствующих эталонах слоев, сформированных на первом этапе моделирования.

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

Исследования позволяют обратить внимание на следующие особенности формализации описанных выше основных этапов подобного компьютерного моделирования. Прежде всего в качестве базовых исходных

данных должны быть заложены важнейшие положения, использованные законодателем при формировании понятия «преступление» в ст. 14 УК, а также положения Общей части УК, 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.

Чтобы обеспечить «технологичность» уголовно-правовой характеристики преступлений рассматриваемого вида в плане расследования соответствующих уголовных дел, в качестве второго основополагающего понятия при формировании системы исходных данных для четвертого этапа компьютерного моделирования преступных проявлений в сфере цифровых прав должна быть использована совокупность признаков понятия «доказательство».

Несмотря на признание многими учеными неразрывных связей уголовного и уголовно-процессуального права, создающих единый правовой фундамент уголовного судопроизводства, на практике они носят в значительной мере формальный характер. В частности, при формировании диспозиций многих уголовно-правовых норм по преступлениям в сфере цифровой экономики должного внимания особенностям их правоприменения с точки зрения положений уголовно-процессуального права не уделялось.

Многие специалисты в качестве причин сложившейся ситуации называли не только существенные различия основных принципов уголовного и уголовно-процессуального права, но и высокую трудность реализации подобных комплексных подходов. Но при надлежащей организации компьютерного моделирования создаются принципиально новые возможности сопряжения положений уголовного и уголовно-процессуального законодательства применительно к преступлениям в сфере цифровой экономики и финансов.

На уровне компьютерного моделирования возможных преступных проявлений рассматриваемого вида выделяется несколько возможных вариантов, имеющих различное содержание. Их условно можно обозначить как «эмпирические», «теоретические» и «комбинированные».

Первый вариант сориентирован на практический опыт выявления, раскрытия и расследования преступлений данного вида. Предварительный анализ показывает, что наибольшее количество соответствующих уголовных дел характерно для мошенничества с использованием электронных средств платежа (ст. 159^3 УК), наименьшее — для манипулирования рынком (ст. 185^3 УК).

При формализации всей совокупности сведений, содержащихся в данных уголовных делах, удастся выделить и систематизировать ха-

рактеристики 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 следователями, прокурорами и судами. По результатам их анализа создадутся возможности сформулировать 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 можно готовить и методические рекомендации для расследования уголовных дел о преступлениях в сфере цифровых прав, включая формирование криминалистических методик.

Теоретические варианты предполагают прежде всего многослойную формализацию правового поля. Что касается комбинированных вариантов, то они 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 варианты смоделированных составов преступлений в сфере цифровых прав, которые выходят за рамки важнейших принципов российского уголовного права.

Заключение

На основе описанных выше юридических алгоритмов возможно в ближайшее время подготовить и отладить пакеты прикладных программ, предназначенных для информационного обеспечения деятельности не только ученых, разрабатывающих проблемы уголовно-правовой защиты субъектов цифровых прав. Они могут использоваться следователями, оперативными сотрудниками, судебными экспертами и специалистами, прокурорами и судьями. Их специфической особенностью является адаптация к применению в интерактивном режиме, который позволяет обеспечить принятие процессуально значимых решений только уполномоченным на это юристом. При этом с помощью проблемно-ориентированного программного обеспечения и баз данных данное лицо получает необходимую информацию в диалоговом режиме с компьютером.

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

Подобные проблемы системного характера зачастую выявляются поздно, когда уголовное дело разваливается при его рассмотрении прокурором или судом. Они нередко провоцируют и трудно выявляемые и трудно исправимые судебные ошибки. Изменить ситуацию даже при использовании подобного программного обеспечения, созданного российскими компьютерными фирмами, крайне трудно.

В то же время детальная разработка иерархических систем юридических алгоритмов позволяет создать их подробное описание, доступное для всех участников уголовного судопроизводства. Это обеспечивает необходимую прозрачность создаваемого на их основе программного обеспечения. Таким образом, 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.

Анализ возможностей реализации описанного комплекса исследований и разработок в сфере уголовно-правовой защиты субъектов цифровой экономики показывает необходимость серьезных организационных усилий, материального и кадрового обеспечения. Аналогичный вывод можно сделать и в отношении разработок, нацеленных на создание необходимого комплекса прикладного программного обеспечения.

Список источников

1. Абдулвадиев А.Ф. и др. Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования. Тюмень: Издательство Тюменского государственного университета, 2021. 376 с.

2. Бычков В.В. Концептуальная, стратегическая и доктринальная основа законодательного противодействия России преступлениям экстремистской направленности, совершенным с использованием ИКТ // Ius Publicum et Privatum. 2022. № 1. С. 166–173.

3. Гаухман Л.Д. Квалификация преступлений: закон, теория, практика. М.: ЮрИнфоР, 2013. 543 с.

4. Головко Л.В. (ред.) Курс уголовного процесса. М.: Статут, 2016, 657 с.

5. Ефимова Л.Г. Источники правового регулирования общественных отношений в киберпространстве // Lex Russica. 2020. № 3. С. 114–120.

6. Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Международный опыт. М.: Международные отношения, 2020. 288 с.

7. Лапин В.О. Научные основы расследования преступлений в сфере предпринимательской деятельности. М.: Юрлитинформ, 2022. 360 с.

8. Лузгин И.М. Моделирование при расследовании преступлений. М.: Юрид. лит., 1981. 152 с.

9. Максимов С.В. и др. Цифровая криминология как инструмент борьбы с организованной преступностью // Всероссийский криминологический журнал. 2018. № 4. С. 476–483.

10. Опальский А.П. (ред.) Уроки правоприменительной практики борьбы с манипулированием рынком. Научно-практическое пособие. М.: Альпен-Принт, 2022. 100 с.

11. Романовский М.Ю., Романовский Ю.М. Математические начала эконофизики. М: Институт компьютерных исследований, 2020. 360 с.

12. Савенко Н.Е. Legaltech в цифровой экономике и правовом регулировании экономической деятельности граждан // Право. Журнал Высшей школы экономики. 2023. Том 16. № 1. С. 145–171.

13. Талапина Э.В. Обработка данных при помощи искусственного интеллекта и риски дискриминации // Право. Журнал Высшей школы экономики. 2022. № 1. С. 4–27.

14. 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. № 2. С. 21–30.

15.Шмонин А.В. Некоторые тенденции развития криминалистических алгоритмов принятия решений в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. № 4. С. 73–77.

16. Янковский Р.М. Криптовалюты в российском праве: суррогаты, «иное имущество» и цифровые деньги // Право. Журнал Высшей школы экономики. 2020. № 4. С. 43–77.

References

1. Abdulvaliev A.F. et al. (2021) Crimes using information technology: qualification and features of investigation. Tyumen: University Press, 376 p. (in Russ.)

2. Bychkov V.V. (2022) Conceptual, strategic and doctrinal basis of legislative counteraction in Russia to extremist criminals using information and telecommunication networks. *Zhurnal chastnogo i publichnogo prava*=Ius Publicum et Privatum, no. 1, pp. 166–173 (in Russ.)

3. Efimova L.G. (2020) Sources of legal regulation of public relations in cyberspace. *Lex Russica*, no. 3, pp. 114–120 (in Russ.)

4. Gaukhman L.D. (2013) *Qualification of crimes: law, theory, practice.* Moscow: Yurinfor, 543 p. (in Russ.)

5. Golovko L.V. et al. (2016) The course of criminal procedure. Moscow: Statut, 657 p. (in Russ.)

6. Lapin V.O. (2022) Theoretical basics of investigation in the field of entrepreneurial activity. Moscow: Yurlitinform, 360 p. (in Russ.)

7. Luzgin I.M. (1981) *Modeling investigation of crimes.* Moscow: Juridicheskaya literatura, 152 p. (in Russ.)

8. Maksimov S.V. et al. (2018) Digital criminology as a tool for combating organized crime. *Rossiyskiy kriminologicheskiy zhurnal*=Russian Journal of Criminology, no. 4, pp. 476–483 (in Russ.)

9. Opalsky A.P. et al. (2022) Lessons from the combating market manipulation: a manual. Moscow: Alpen-Print, 100 p. (in Russ.)

10. Romanovsky M.Yu., Romanovsky Yu. M. (2020) Mathematical principles of economophysics: a manual. Moscow: Institute of Computer Research, 360 p. (in Russ.)

11. Savenko N.E. (2023) Legaltech in the digital economy and legal regulation of economic activity of citizens. *Pravo*. *Zhurnal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, vol. 16, no. 1, pp. 145–171 (in Russ.)

12. Shmonin A.V. (2017) Trends in forensic decision-making algorithms in criminal proceedings.*Trudy akademii upravlenia MVD*=Works of the Academy of Management of Internal Ministry, no. 4, pp. 73–77 (in Russ.)

13. Talalina E.V. (2022) Data processing using artificial intelligence and the risks of discrimination. *Pravo*. *Zhurnal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, vol. 15, no. 1, pp. 4–27 (in Russ.)

14. Timoshenko A.A., Feyzov V.R., Chernov I.V. (2023) Scenario approach to the study of regulation in the field of cryptocurrencies in Russia. *Rossiyskiy zhurnal pravovykh issledovaniy*=Russian Journal of Legal Studies, no. 2, pp. 21–30 (in Russ.)

15. Yankovsky R.M. (2020) Cryptocurrencies in Russian Law: Surrogates, “other property” and digital money. *Pravo*. *Journal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, vol. 14, no. 4, pp. 43–77 (in Russ.)

16. Zhdanov Yu.N., Ovchinsky V.S. (2020) *Cyberpolice of the 21th century: international experience.* Moscow: Mezhdunarodnye otnoshenia, 288 p. (in Russ.)

Информация об авторах:

С.В.Расторопов — доктор юридических наук, профессор.

В.А. Прорвич — доктор юридических наук, доктор технических наук, профессор-исследователь.

Information about the authors:

S.V. Rastoropov — Doctor of Sciences (Law), Professor.

V.A. Prorvich — Doctor of Sciences (Law), Doctor of Sciences (Technology), Professor-Researcher.

Статья поступила в редакцию 09.04.2024; одобрена после рецензирования 30.04.2024; принята к публикации 03.05.2024.

The article was submitted to editorial office 09.04.2024; approved after reviewing 30.04.2024; accepted for publication 03.05.2024.