Право. Журнал Высшей школы экономики. 2025. Том 18. № 2.
Law. Journal of the Higher School of Economics. 2025. Vol. 18, no 2 .

Научная статья
JEL:K1
УДК: 343.1
DOI:10.17323/2072-8166.2025.2.190.218

Юридические алгоритмы формирования предмета доказывания по преступлениям в сфере цифровой экономики и финансов

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

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

[1] vprorvich@hse.ru, https://orcid.org/0009-0000-5964-9056

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

Аннотация

Для надлежащего правоприменения по преступлениям в сфере цифровой экономики и финансов особое значение имеет использование взаимных связей уголовного и уголовно-процессуального законодательства, создающих единый правовой фундамент уголовного судопроизводства. В статье раскрываются особенности применения определенных совокупностей положений действующего законодательства в форме юридических алгоритмов, надлежащее использование которых позволяет сформировать развернутую характеристику предмета доказывания, а также применить системы юридических тождеств для их использования при установлении пределов доказывания по соответствующим уголовным делам. Описаны научно обоснованные подходы к установлению структуры и содержания информации, имеющей правовой статус, в каждом из доказательств, полученных при расследовании уголовных дел. На их основе разработаны алгоритмы представления доказательств в виде одномерных и многомерных матриц, содержание которых стандартизовано на основе признаков составов преступлений рассматриваемого вида и обстоятельств, подлежащих доказыванию по данным уголовным делам. Это позволяет выполнить их надлежащую проверку и оценку, а также уста-

новить достаточность собранной совокупности доказательств. В информационную структуру таких юридических алгоритмов имплементированы «простые» системы юридических тождеств, ориентированных на установление достаточности данных, которые соответствуют признакам состава преступления (что позволяет принять решение о возбуждении уголовного дела), а также «двойные» системы юридических тождеств, позволяющих установить достаточность собранной совокупности доказательств на различных стадиях расследования уголовного дела. Раскрыты особенности иерархических систем юридических алгоритмов, разработанных для выявления признаков совершенных совокупностей преступлений в сфере экономики и компьютерной информации с «перекрестными» формами соучастия. Они нацелены на выявление по результатам расследования соответствующих составов преступлений, совершенных каждым из соучастников. Обсуждаются подходы к научному обоснованию предложений о внесении изменений и дополнений в часть шестую УПК, регламентирующих порядок обработки электронной информации с использованием сертифицированного программного обеспечения для получения доказательств и доказывания по преступлениям в сфере цифровых прав.

Ключевые слова

цифровые права; киберпреступления; юридические алгоритмы; доказывание; информационный формат доказательств; юридические тождества; интерактивные информационные системы.

Для цитирования: Прорвич В.А., Расторопов С.В. Юридические алгоритмы формирования предмета доказывания по преступлениям в сфере цифровой экономики и финансов // Право. Журнал Высшей школы экономики. 2025. Том 18. № 2. С. 190–218. DOI:10.17323/2072-8166.2025.2.190.218

Research article

Legal Algorithms for the Formation of the Subject of Evidence for Crimes in the Field of Digital Economy and Finance

Vladimir A. Prorvich[1], Sergey V. Rastoropov[2]

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

[1] vprorvich@hse.ru, https://orcid.org/0009-0000-5964-9056

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

Abstract

For proper law enforcement in crimes in the field of digital economy and finance, the use of mutual connections between criminal and criminal procedural legislation, creating a unified legal foundation for criminal proceedings, is of particular importance. The article reveals the features of the application of certain sets of provisions of the current

legislation in the form of legal algorithms, the proper use of which allows to form a detailed description of the subject of proof, as well as to apply systems of legal identities for their use in establishing the limits of proof in relevant criminal cases. Scientifically based approaches to establishing the structure and content of information that has a legal status in each of the evidence obtained during the investigation of criminal cases are described. On their basis, algorithms for presenting evidence in the form of one-dimensional and multidimensional matrices have been developed, the content of which is standardized based on the features of the crimes of the type under consideration and the circumstances subject to proof in these criminal cases. This allows for their proper verification and assessment, as well as establishing the sufficiency of the collected set of evidence. The information structure of such legal algorithms implements "simple" systems of legal identities aimed at establishing the sufficiency of data that correspond to the signs of the crime (which allows making a decision to initiate a criminal case), as well as "double" systems of legal identities that allow establishing the sufficiency of the collected set of evidence at various stages of the criminal case investigation. The features of hierarchical systems of legal algorithms developed to identify signs of committed sets of crimes in the sphere of economics and computer information with "cross" forms of complicity are disclosed. They are aimed at identifying, based on the results of the investigation, the corresponding crimes committed by each of the accomplices. Approaches to the scientific substantiation of proposals to amend and supplement to Part 6 of the Criminal Procedure Code regulating the procedure for processing electronic information using certified software for obtaining evidence and proving crimes in the field of digital rights are discussed.

Keywords

digital rights; cybercrimes; legal algorithms; evidence; information format of evidence; legal identities; interactive information systems.

For citation: Prorvich V.A., Rastoropov S.V. (2025) Legal Algorithms for the Formation of the Subject of Evidence for Crimes in the Field of Digital Economy and Finance. *Law. Journal of the Higher School of Economics*, vol. 18, no. 2, pp. 190–218 (in Russ.) DOI:10.17323/2072-8166.2025.2.190.218

Введение

Создание надежной системы уголовно-правовой защиты современных общественных отношений в весьма сложных условиях перехода к информационному обществу и экономике знаний[1] предпо-

[1] Стратегия развития информационного общества Российской Федерации на 2017–2030 годы, утверждённая 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 Консультант Плюс.

лагает внесение корректировок и дополнений в определенные главы Уголовного кодекса Российской Федерации (далее — УК) и Уголовно-процессуального кодекса Российской Федерации (далее — УПК), а также в ряд других федеральных законов и подзаконных актов. Их надлежащее обоснование требует коллективных усилий ученых, изучающих различные сферы наук уголовно-правового и информационного блоков.

В первую очередь речь идет об уголовно-правовых нормах, включенных законодателем в 21, 22, 23 и 28 главы УК, в рамках которых криминализована большая часть общественно опасных деяний в различных сферах цифровой экономики и финансов. Как показывает анализ правоприменительной практики, преступность в данных сферах отличаются не только высокими темпами роста, но высоким уровнем латентности. Особенно острая ситуация сложилась при совершении новых видов мошенничества с электронными средствами платежа, а также различных видов манипулирования рынком.

Эмиссионные ценные бумаги выпускаются и обращаются только в форме электронных документов с помощью цепочек информационных систем профессиональных участников фондового рынка, контролируемого Банком России. Однако на протяжении 12 лет после криминализации соответствующих деяний выявлялось в среднем одно подозрительное событие в месяц, возбуждались уголовные дела в среднем по каждому четвертому событию, а приговоры суда выносились менее одного раза в год [Опальский А.П., 2022: 3–10].

Одной из причин ситуации является недостаточное внимание к прогнозированию будущей деятельности юристов-правоприменителей при криминализации все более сложных по своей структуре и содержанию общественно опасных деяний в сфере цифровых прав. При этом даже понятие общественной опасности применительно к условиям перехода к информационному обществу и экономике знаний раскрыто пока далеко не полностью.

Требует принципиально нового осмысления и ряд установок, отражающих прямые и обратные связи ключевых положений кодифицированного законодательства и создающих правовой фундамент российского уголовного судопроизводства [Головко Л.В., 2016: 5–7]. В позиции некоторых наших коллег нередко проявляется стремление к ориентации на философские основы уголовного права, незыблемость фундаментальных определений и т.п. Вместе с тем другие коллеги делают упор на особенностях деятельностного подхода к выявлению наиболее актуальных проблем современного уголовного судопроизводства применительно к борьбе с киберпреступностью и

разработке способов их решения [Абдулвадиев А.Ф., 2021: 39–54]. Это дает им основание для поиска альтернативы позитивному праву в рамках различных подходов к пониманию «реального» права.

Для раскрытия содержательных особенностей происходящих общественных процессов представителям юридических наук уголовно-правового блока важно найти способы имплементации инструментария, созданного в рамках наук информационного блока, не выходя при этом за рамки уголовного и уголовно-процессуального права. Исследования позволили раскрыть принципиально новые возможности для совершенствования российской правовой системы в условиях перехода к информационному обществу и экономики знаний. В данном контексте настоящая статья продолжает рассмотрение этих возможностей, которые уже обсуждались в нашей предыдущей статье в данном журнале.

Некоторые из них связаны с формированием на основе определенных групп правовых норм юридических алгоритмов различного вида и назначения. Для этого используются многомерные матрицы с прямыми и обратными связями групп правовых норм и понятий, сформированных на их основе, а также простые и двойные системы юридических тождеств. В результате создаются возможности разработки и исследования информационно-математических моделей проблемно-ориентированного характера, раскрывающих важнейшие особенности современных криминальных явлений и позволяющих сформировать обширную систему разнообразных «информационных эталонов». Это открывает ряд принципиально новых возможностей в использовании позитивного права для эффективной защиты субъектов цифровых прав [Волынский А.Ф., 2019: 260–271].

В качестве одной из наиболее актуальных проблем в ряде работ обсуждается создание научно обоснованного фундамента для создания юридического алгоритмического языка, обеспечивающего переход на новый уровень взаимопонимания юристов и специалистов в сфере информатики [Волынский А.Ф., 2020: 215]. Ее решение осложняется не только необходимостью создания лексических единиц, правил их использования и словаря. Важно понимать и особенности неразрывных связей языка и мышления в различных сферах человеческой деятельности.

Отнюдь не зря родилось крылатое выражение: «два юриста — три мнения». Оно отражает особенности не только их деятельности, но и способа мышления, ориентированного на раскрытие многозначности многих из используемых ими понятий исходя из установок

юридической школы и собственного опыта, открывающих широкие возможности для их толкования.

Эта ситуация особенно ярко проявилась в последние годы, когда на смену парадигме рыночного капитализма с рядом постулатов саморегулирования экономики и финансовой системы государства стало приходить понимание незаменимой роли государства в социально-экономическом развитии страны. К этому добавились и принципиально новые для юристов процессы всеобщей цифровизации современного общества, ключевую роль в управлении которыми играют владельцы крупных фирм, обеспечивающих государство и общество сетевым оборудованием, компьютерной техникой, а также системным и прикладным программным обеспечением.

Характерным примером подобного правотворчества является внесение в ряд статей Гражданского кодекса Российской Федерации (далее — ГК) дополнений, отражающих изменение структуры и содержания имущественных прав. В частности, речь идет о новом виде обязательственных прав, названных цифровыми правами, содержание которых и условия их осуществления определяются в соответствии с правилами информационной системы[2].

Несмотря на использованное в названии данного вида прав понятия «цифровые», при раскрытии этого понятия в нескольких статьях ГК понятие «цифра» вообще не используется. Вместо манипулирования цифрами законодатель дает развернутые описания порядка использования в правоотношениях субъектов различного вида и уровня нового вида обязательственных прав. Поскольку ответственность обладателей информационных систем за несоответствие установленных ими правил требованиям законодательства не предусмотрена, а также из-за нестыковок правил взаимосвязанных информационных систем различного вида и назначения возникает и ряд правовых коллизий нового вида.

Одним из примеров таких коллизий стало введение понятия «цифровые финансовые активы»[3], поскольку они были определены как 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.

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

[3] Федеральный закон № 259-ФЗ от 31.07.2020 // СПС КонсультантПлюс.

Поскольку правила иностранных информационных систем не связаны с российским законодательством, это создает дополнительные проблемы при выявлении правонарушений и преступлений в данной сфере. Многие из них связаны с использованием субъектами цифровых прав различных видов электронных документов и разнообразного программного обеспечения, а разработка соответствующих процессуальных норм, как отмечалось выше, сильно затянулась.

Для разработки надлежащего применения уголовно-правовых норм по преступлениям в сфере цифровой экономики и финансов необходимы исследования по созданию проблемно-ориентированного программного обеспечения, создающего не только возможность получения информации, имеющей значение для уголовного дела. Речь идет и о необходимости использования специальных технологий для надлежащего контроля за сохранением правового статуса промежуточных и итоговых результатов обработки электронных документов. Кроме того, информационно-математические модели и алгоритмы обработки информации должны быть формализованы таким образом, чтобы обеспечить возможность надлежащей проверки и оценки результатов обработки информации с помощью создаваемого программного обеспечения.

Данная работа нацелена на раскрытие обозначенных проблем формирования уголовно-правовой защиты субъектов цифровых прав в различных сферах современной экономики и финансов, а также новых подходов к их решению. В их основу заложены методы информационно-правового моделирования предмета доказывания по уголовным делам о преступлениях рассматриваемого вида, а также системы юридических алгоритмов для установления пределов доказывания.

Это позволит создать проблемно-ориентированное, выверенное с правовой точки зрения программное обеспечение, ориентированное на надлежащее применение интерактивных информационных систем, необходимых для выявления и фиксации закодированных информационных следов в электронной документации, связанной с преступлениями рассматриваемого вида. Поскольку для многих из них, включая манипулирование рынком эмиссионных ценных бумаг и производных финансовых инструментов, характерно использование новых криминальных способов воздействия на высокоинтенсивные потоки документированной информации, такие виды преступлений приобретают свойства киберпреступлений в сфере экономики.

Для их выявления, раскрытия и расследования необходима разработка принципиально новых информационных технологий, вы-

веренных с правовой точки зрения, основанных на оригинальных математических методах анализа и управления интенсивными потоками документированной электронной информации с выявлением и фиксацией криминальных событий. Использование математического аппарата для их описания обеспечивает последующее надлежащее выполнение процессуально регламентированных действий по надлежащему формированию совокупности доказательств по результатам обработки высокоинтенсивных потоков электронных документов и иной электронной информации, характерных для киберпреступленнй рассматриваемого вида.

Решение важнейших проблем на стыке уголовного, уголовно-процессуального права, кибернетики и информатики позволяет не только формировать информационные модели предмета доказывания по киберпреступлениям в сфере цифровой экономики. На их основе могут быть разработаны юридические алгоритмы обработки электронных документов и интерактивные информационные системы с соответствующим проблемно-ориентированным программным обеспечением и информационными эталонами различного вида и назначения, позволяющие следователю выполнять оперативный контроль за сохранением правового статуса электронной информации по соответствующим уголовным делам.

1. Юридические алгоритмы формирования предмета доказывания по киберпреступлениям в сфере цифровой экономики

Как показывает обобщение сложившейся за последние годы правоприменительной практики, уголовно-правовое познание криминальных событий для выполнения соответствующих действий, предусмотренных уголовным и уголовно-процессуальным законодательством, всегда ретроспективно. Кроме этого, оно формализовано на основе соответствующих положений УПК и неразрывно связано с установками УК, а также отличается цикличностью и возобновляемостью [Головко Л.В., 2016: 8–9].

Что касается раскрытия соответствующих особенностей уголовно-правового познания по киберпреступлениям в сфере экономики, то в литературе подробно обсуждаются ситуации, связанные с мошенничеством с электронными средствами платежа различного вида, незаконным кредитованием, незаконной банковской деятельностью, преднамеренным банкротством, коррупционными схемами с использованием криптовалюты и многими другими преступлени-

ями в сфере цифровой экономики и финансов [Жданов Ю.Н., 2020: 16–18].

Для каждого из подобных преступлений можно выделить ряд особенностей в способах их подготовки, совершения и сокрытия, включая использование разнообразных технических средств и программного обеспечения. Во многих случаях отмечаются разнообразные сочетания новых, высокотехнологичных приемов из арсенала современного криминала с традиционными приемами, используемыми в течение многих десятилетий. Особенно острая ситуация сложилась по преступлениям в сфере манипулирования рынком, уголовная ответственность за совершение которых предусмотрена ст. 185^3 УК, включая высочайший уровень их латентности [Опальский А.П., 2022: 11–15].

Подчеркнем, что раскрытие уголовно-правовых аспектов информационного содержания киберпреступлений в сфере экономики, их совокупностей, а также уголовно наказуемых приготовлений к их совершению требует обширных исследований и разработок. Детальному анализу возможностей использования нового инструментария для информационно-математического моделирования криминальных проявлений в сфере цифровой экономики и финансов при разработке наиболее эффективных методик борьбы с киберпреступлениями данного вида посвящены другие наши научные исследования, а также работы наших коллег [Бастрыкин А.И., 2023: 105–113].

В данной статье, опираясь на важнейшие особенности единого информационного содержания уголовно-правовых и уголовно-процессуальных понятий с точки зрения объективных потребностей уголовного судопроизводства, авторы рассматривают ряд новых подходов к разработке современного инструментария на основе юридических алгоритмов, обеспечивающего надлежащее формирование предмета доказывания по киберпреступлениям.

Раскрывая особенности предмета доказывания по киберпреступлениям в сфере экономики, многие специалисты делают акцент на детализации целевой установки доказательственного права — установление состава преступления и обстоятельств, подлежащих доказыванию. При совершении совокупностей киберпреступлений в сфере экономики с различными формами соучастия, формирование информационно полной системы обстоятельств, подлежащих доказыванию, значительно труднее. Прежде всего это связано с тем, что приходится учитывать наличие совокупностей обязательных и факультативных признаков нескольких составов преступлений.

Многие из них являются многоэпизодными и совершаются в течение длительного времени, а промежутки времени, в течение ко-

торых они «пересекаются» и образуют совокупности, могут быть установлены лишь в процессе расследования уголовного дела. Кроме того, проблемы формирования обстоятельств, подлежащих доказыванию, и установление их связей с составами преступлений, характеризующих уголовно наказуемые приготовления к киберпреступлениям рассматриваемого вида, также разработаны пока в недостаточной степени для их надлежащего правоприменения [Бастрыкин А.И., 2023: 115–134].

Рассмотрение особенностей соответствующих информационных технологий, разрабатываемых на основе совокупностей юридических алгоритмов, позволяющих раскрыть важнейшие особенности понятий «доказательство», «предмет доказывания», «пределы доказывания», позволяет сделать следующие выводы.

В соответствии с определением понятия «доказательство», установленным законодателем в ч. 1 ст. 74 УПК, речь идет о «сведениях», то есть о виде информации, имеющей специфическое, правовое содержание, отражающее особенности обстоятельств, подлежащих доказыванию при производстве по уголовному делу о преступлении, а также иных обстоятельств, имеющих значение для уголовного дела. Как уже отмечалось выше, в соответствии с требованиями ст. 24 УПК речь идет об информации, позволяющей установить в деянии все признаки состава данного преступления [Бастрыкин А.И., 2016: 15–29].

Анализ совокупности приведенных выше правовых установлений показывает, что с информационно-правовой точки зрения фактически речь идет о введении законодателем системы алгоритмов юридически регламентированных действий уполномоченных на то законом лиц, нацеленных на формирование системы сведений строго определенного уголовно-процессуальным законодательством содержания, позволяющих на их основе суду принять решение, предусмотренное законодательством. Понятно, что в контексте развития процессов перехода к информационному обществу и экономике знаний, раскрытие особенностей всей совокупности данных юридических алгоритмов приобретает большое значение.

Указанные процессуальные действия могут выполняться только строго ограниченным кругом лиц — судьями, прокурорами, следователями и дознавателями. При этом законодатель установил ограничения на свободу действий указанных лиц, указав на их выполнение в порядке, определенном настоящим Кодексом, а также регламентировал особенности их правоотношений в рамках соответствующих процессуальных действий с представителями стороны защиты.

Даже без рассмотрения деталей процессуально регламентированных действий указанных лиц, допустимо сделать обоснованный вывод: создаваемые ими юридические алгоритмы на основе одних и тех же уголовно-процессуальных норм могут существенно различаться в силу возложенных на них обязанностей. Дополнительные различия возникают и в процессе их реализации, в том числе вследствие существенного различия индивидуальных качеств этих лиц. Соответственно возникает необходимость постановки и выполнения научных исследований для разработки основных принципов, на основе которых могут быть созданы стандарты формирования таких юридических алгоритмов в свете отмеченных субъективных факторов.

Но это позволит решить лишь часть проблем, связанных с надлежащим формированием и применением подобных юридических алгоритмов, которые носят проблемно-ориентированный характер. То есть они нацелены на получение не любой информации, имеющей значение для расследования указанных уголовных дел, а строго конкретизированной законодателем. Речь идет о таких сведениях, которые позволяют установить в подозрительном деянии обстоятельства, подлежащие доказыванию, и признаки состава данного преступления. При этом обращение к положениям ст. 8 УК показывает, что должны быть установлены все признаки состава преступления, а не их часть.

Результаты исследований показывают, что описанная выше система юридических алгоритмов обеспечивает возможность формирования развернутой уголовно-правовой характеристики как отдельных киберпреступлений в сфере экономики, так и их совокупностей, совершенных с различными формами соучастия, а также уголовно наказуемых приготовлений к таким преступлениям. При этом могут накладываться проблемы использования субъективно выбранных положений гражданского и специального законодательства, а также параллельного раскрытия нескольких бланкетных диспозиций тех преступлений, которые образуют соответствующие совокупности [Гаухман Л.Д., 2013: 175–181].

Важную роль здесь может сыграть анализ особенностей составов преступлений данного вида, завершенных расследованием и рассмотренных судом с вынесением обвинительных приговоров. Это позволит не только «приземлить» научно-теоретические разработки в данном направлении, но и выявить возможные неточности в идентификации составов киберпреступлений рассматриваемого вида в рамках правоприменительной практики.

В русле соответствующих информационно-правовых связей данных юридических алгоритмов, а также с применением указанных правовых акцентов они могут быть объединены в единую иерархически выстроенную систему алгоритмов, на основе которой может быть создан соответствующий информационно-технологический инструментарий [Новиков А.М., 2022: 21–27].

2. Юридические алгоритмы получения, проверки и оценки доказательств на основе электронных документов и иных сведений

Выше отмечалось, что каждое доказательство должно содержать проблемно-ориентированную информацию не только об одном или нескольких признаках состава киберпреступления, либо об одном или нескольких обстоятельствах, подлежащих доказыванию при расследовании уголовного дела об этом киберпреступлении, но и об источнике данной информации. Таким образом, необходимо установить наличие единства формальной (ч. 2 ст. 74 УПК) и материальной (содержательной) (ч. 1 ст. 74 УПК) сторон каждого из полученных доказательств.

Как уже отмечалось выше, опираясь на одно из ключевых понятий уголовного судопроизводства — «преступление», при установлении признаков состава преступления в деянии, о котором была получена «инициирующая» информация, следователь или дознаватель сталкиваются с необходимостью выбора способа дальнейших действий. Фактически речь идет о «стартовом сигнале» начала поиско-познавательной деятельности следователя, нацеленной на получение таких сведений, которые позволяют ему доказать, что действительно было совершено преступление.

Ввиду применения для получения доказательств весьма трудоемких и дорогостоящих процедур, информационных технологий, системного и прикладного программного обеспечения, вполне естественным решением государства является принятие на себя обязанностей по сбору, проверке и оценке доказательств по киберпреступлениям в сфере экономики. При этом речь идет не только о доказательствах «обвинительного» характера, но и «оправдательного». К тому же сторона защиты никак не ограничивается в предъявлении доказательств по соответствующим уголовным делам [Володина Л.М., 2024: 195–214].

В этой связи анализ положений ч. 1 ст. 24 УПК показывает, что речь идет о необходимости перманентного выполнения квалифика-

ции преступления в процессе расследования уголовного дела. Здесь критически важным становится понимание динамического характера процесса установления наличия либо отсутствия состава преступления (в пределах установленных законом процессуальных сроков выполнения определенных совокупностей следственных действий). Особенно трудные задачи приходится решать, когда вначале выявляется и расследуется первое преступление из их совершенной совокупности, а затем, в процессе расследования уголовного дела устанавливаются сведения, соответствующие признакам второго состава преступления. Для их решения необходимо использовать специально разработанный инструментарий, особенности которого рассматриваются ниже.

Исследования, нацеленные на обеспечение надлежащего применения инструментария правовой информатики при оперировании понятием «доказательства», а также формирования соответствующих групп юридических алгоритмов различного вида показывают, что необходимо раскрыть важнейшие структурно-содержательные особенности правовой информации, заключенной в доказательствах различного вида.

Всю совокупность доказательств, которые после их надлежащей проверки и оценки должны отвечать требованиям достаточности, установленным ст. 88 УПК, можно представить в виде двух двумерных матриц. Каждая из строк этих матриц — описание информационного содержания доказательства. Каждый из столбцов первой матрицы характеризует содержание одного из признаков состава преступления. Каждый из столбцов второй матрицы характеризует содержание одного из обстоятельств, подлежащих доказыванию по расследуемому уголовному делу.

Соответственно каждая из строк первой матрицы представляет собой одномерную матрицу, количество элементов которой соответствует количеству признаков состава расследуемого преступления. При этом в некоторых из данных одномерных матриц может быть заполнен лишь один из элементов, соответствующий одному из признаков состава данного преступления, а остальные элементы — пустые. В других — два элемента, соответствующие двум признакам состава этого преступления, и даже большее количество элементов. Понятно, что чем больше элементов оказываются заполненными, тем более информативным является данное доказательство [Новиков А.М., 2022: 29–33].

К примеру, в протоколе допроса потерпевшего, с дебетовой карты которого бывшим сотрудником банка с помощью сообщника-программиста похищена крупная сумма, могут содержаться сведения

о размере причиненного ему ущерба, т.е. о предмете преступления и о последствиях этого деяния. В протоколе допроса подозреваемого могут быть зафиксированы сведения о времени, месте, способе совершения данного преступления, личности его сообщника, их образовании и практическом опыте, раскрывающих признаки специальных субъектов, а также формы их вины. Следовательно, в первой одномерной информационной матрице, характеризующей уголовно-правовое содержание первого доказательства, могут быть заполнены лишь два элемента, а во второй — не менее шести. То есть второе доказательство обладает в три раза большей «информационной емкостью», чем первое.

Вместе с тем сравнительный анализ содержательных особенностей определений, использованных законодателем для доказательств различного вида, указывает на ряд их смысловых различий. В частности, в ст. 81 УПК законодатель определил вещественные доказательства как предметы различного вида, которые приобщаются к уголовному делу и хранятся в порядке, предусмотренном данной статьей и ст. 82.

Таким образом, в отличие от базового определения доказательства, установленного в ч. 1 ст. 74 УПК, в котором речь идет о сведениях определенного правового содержания и назначения, т.е. о специализированной информации, при определении вещественного доказательства законодатель уже ведет речь о предмете, а не о сведениях или информации об этом предмете. Это создает ряд проблем при выполнении следователем проверки «текстовых» и вещественных доказательств путем их взаимного сопоставления, как это предусмотрено ст. 87 УПК. Подобные проблемы возникают и при определении достаточности собранной следствием совокупности доказательств, что предусмотрено ст. 88 УПК.

Анализ соответствующих положений действующего законодательства показывает, что в простых ситуациях для этого могут использоваться протоколы осмотра следователем вещественных доказательств. В сложных ситуациях нередко возникает необходимость использования знаний привлеченных для этого следствием специалистов. В наиболее трудных случаях для раскрытия информационного содержания вещественных доказательств могут использоваться специальные знания судебных экспертов, в том числе в форме комплексных судебных экспертиз с привлечением экспертов разных специальностей.

Но важно, что при раскрытии информационного содержания вещественных доказательств с применением специальных знаний

в указанных выше процессуальных формах соответствующий «информационный образ» вещественного доказательства, описанный в протоколе осмотра, заключении специалиста или в заключении эксперта, является новым доказательством, относящимся к другому виду, установленному ч. 2 ст. 74 УПК.

В результате фактически происходит формирование «парного», «двойного» или «двустороннего» доказательства, в основе которого находится предмет, имеющий значение для уголовного дела, а система сведений об обстоятельствах, подлежащих доказыванию, а также об обязательных и факультативных признаках состава преступления, то есть его информационно-правовое содержание отражено в соответствующем протоколе, заключении эксперта или специалиста. При этом предъявление юридически значимых характеристик вещественного доказательства в том же информационно-правовом формате, что и доказательства других видов, позволяет обеспечить его проверку и оценку в соответствии с правилами, установленными ст. 87 и 88 УПК.

Чаще всего необходимость в раскрытии информационно-правового содержания вещественного доказательства при выполнении следственных действий с носителями электронной информации. При этом вновь появляется необходимость приведения содержащихся в них сведений к единому информационному формату. Для «считывания» информации с ее электронного носителя нередко оказывается достаточным провести его следственный осмотр или привлечь специалиста, владеющего необходимыми профессиональными компетенциями использования одной из имеющихся в его распоряжении компьютерных программ. Но во многих случаях необходима судебная экспертиза с привлечением ученых и специалистов, занимающихся искусственными алгоритмическими языками, а также применением для решения подобных экспертных задач искусственного интеллекта. До начала проверки данного «вещественного» доказательства приходится сперва обеспечить проверку и оценку заключения специалиста или заключения эксперта, соответственно, решив при этом ряд новых проблем.

Поскольку система алгоритмов, на основе которых была создана использованная экспертом компьютерная программа, самому эксперту не известна, то в рамках экспертных исследований он не может сформировать и описать свою методику на языке, понятном следователям, прокурорам, судьям, присяжным заседателям, на которых возложены обязанности проверки и оценки заключения эксперта как доказательства по уголовному делу. Тем самым он лишает указанных лиц возможности выполнить обязательные требования

ряда положений УПК. В результате из-за нарушения требований п. 9 ч. 1 ст. 204 УПК соответствующие заключения экспертов-программистов должны быть признаны недопустимыми доказательствами, как этого требует ст. 75 УПК, со всеми вытекающими из этого последствиями.

Здесь со всей остротой еще раз встает проблема неоконченного правотворчества в рамках части шестой УПК. Из-за этого уголовное судопроизводство до сих пор не обеспечено современным информационно-технологическим инструментарием, выверенным с правовой точки зрения. Формирование соответствующих уголовно-процессуальных норм позволило бы обеспечить получение необходимых доказательств и доказывание по киберпреступлениям в сфере экономики на основе электронных документов и иной электронной информации с использованием для этого сертифицированных надлежащим образом компьютерных программ.

В основу разработок, нацеленных на решение этих проблем, может быть положен накопленный в последние годы опыт формирования системы юридических алгоритмов преобразования соответствующей информации, созданных на основе применения совокупностей уголовно-процессуальных норм в сочетании с рядом положений уголовного права. Подобные юридические алгоритмы могут быть выстроены в иерархические системы, нацеленные на выполнение обширного комплекса алгоритмического преобразования исходной информации, имеющей значение для уголовного дела о преступлениях рассматриваемого вида, включая организацию контроля над сохранением правового статуса промежуточных и итоговых результатов обработки исходной информации.

Безусловно, как показывает анализ тенденций в использовании современных информационных технологий во всех сферах общественных отношений, важно понимать особенности применения в уголовном судопроизводстве различных программных комплексов с использованием элементов искусственного интеллекта [Талапина Э.В., 2022: 4–27]. Однако для существенного снижения рисков нарушения основных принципов уголовного права из-за попыток навязывания технократических подходов при использовании обширных комплексов разнообразных компьютерных программ необходимо принятие специальных мер. При этом важную роль может сыграть разработка научно обоснованных и выверенных с правовой точки зрения требований к архитектуре и функциям интерактивных информационных систем, основанных на применении совокупностей юридических алгоритмов.

Для обработки юридически значимой информации в их структуре можно выделить формирование логически выстроенной системы «коротких» алгоритмов обработки электронной информации. Это позволяет следователю на более высоком уровне понимания контролировать содержательные особенности промежуточных результатов, полученных на каждом шаге выполнения преобразований исходной информации, заложенных соответствующим алгоритмом, а также сохранение их правового статуса.

В рамках надлежащим образом организованного диалога со своим компьютерным помощником следователь может получать самую различную справочную информацию, выполнить сравнительный анализ различных вариантов применения положений законодательства, получить несколько вариантов результатов обработки определенных сведений с помощью искусственного интеллекта и т.п. Таким образом он получает возможность принятия надлежащим образом обоснованного решения о придании правового статуса полученным результатам и скрепления его своей электронной подписью.

Следует подчеркнуть, что алгоритмы формирования различных доказательств на основе результатов обработки следователем документированной электронной и иной информации могут существенно различаться. Это отмечалось еще на ранних стадиях применения компьютеров при расследовании преступлений [Соя-Серко Л.А., 1980: 33–34]. Степень их адекватности задачам, которые необходимо решить при расследовании уголовного дела, зависит от различных факторов, в том числе от различной «информационной емкости» доказательств, одни из которых позволяют идентифицировать в квалифицируемом деянии лишь один признак состава преступления или одно обстоятельство, подлежащее доказыванию, а другие — несколько таких признаков или обстоятельств. Кроме того, при обработке информации, на основе которой происходит формирование доказательств следствием, важно видеть особенности ее фиксирования на бумажных и электронных носителях, в графической, текстовой и числовой формах, а также иные ее структурно-содержательные особенности, которые могут существенно осложнить не только их проверку и оценку, но и установление достаточности их собранной совокупности.

Что касается проверки доказательств путем их сопоставления, то речь идет о части юридических алгоритмов, которые обеспечивают возможность их «параметрического» сопоставления по совпадающим элементам одномерных информационных матриц, аппроксимирующих их правовое содержание. Другая часть юридических ал-

горитмов с соответствующей системой информационных эталонов может применяться для оценки доказательств по установленным ст. 88 УПК критериям.

3. Юридические алгоритмы для установления пределов доказывания на различных стадиях досудебного производства

В рамках доказательственного права понятие предмета доказывания по уголовным делам о конкретных преступлениях неразрывно связано с понятием пределов доказывания [Тимошенко А.А., 2016: 114–120]. В свою очередь для установления пределов доказывания в уголовно-процессуальном праве неоднократно используется такой критерий информационного характера, как «достаточность». При этом данный критерий применяется и в сочетании с понятием «данные» (ч. 2 ст. 140 УПК) при решении вопроса о возбуждении уголовного дела, и с понятием «сведения» (ч. 1 ст. 74, ч. 2 ст. 153, ст. 171 и 215 УПК) на различных стадиях расследования уголовного дела.

Практическое применение этих положений уголовно-процессуального законодательства существенно осложняется из-за того, что ни в перечисленных выше, ни в других статьях УПК законодатель не раскрыл содержательных особенностей критически важного для процесса доказывания критерия достаточности соответствующих данных и сведений. Не раскрыт и порядок выполнения процессуально регламентированных действий для установления того, выполняется данный критерий или нет [Дикарев И.С., 2017: 117–122].

Необходимо еще раз обратить внимание на особенности информационно-правовых аспектов понятий «данные» и «сведения», которые раскрываются в отмеченных выше положениях УПК. На их основе разработаны «простые» и «двойные» системы юридических тождеств, используемые в рамках соответствующих юридических алгоритмов. Это позволяет оказать надлежащую информационную поддержку следователям, другим участникам уголовного судопроизводства и судам в практическом применении данного критерия при реализации одного из важнейших принципов — свободы оценки доказательств.

Простые системы юридических тождеств используются в составе юридических алгоритмов, обеспечивающих установление достаточности полученных следствием данных для возбуждения уголовного дела. В таких системах количество юридических тождеств определяется количеством признаков состава данного преступления. В их

левую часть помещается описание одного из признаков состава преступления, а в правую — данные, раскрывающие содержание поводов для возбуждения уголовного дела, указанных в ст. 141–143 УПК. В рамках данных алгоритмов также предусмотрена возможность приведения полученных данных к единому информационному формату [Новиков А.М., 2022: 76–80].

Анализ особенностей сформированной системы юридических тождеств позволяет следователю установить, имеется ли в квалифицируемом деянии состав преступления, соответствующий установкам ст. 8 УК. Его результаты дают возможность сделать и ряд дополнительных выводов по обсуждаемым проблемам. Установить выполнение каждого юридического тождества в их простой системе удается далеко не всегда. Достаточно привести многочисленные примеры, когда уголовное дело возбуждается по факту совершения преступления, когда данных о субъекте преступления либо недостаточно, либо они отсутствуют. Естественно, что в таких случаях отсутствуют данные и о субъективной стороне преступления [Стойко Н.Г., 2014: 168–173].

Вместе с тем нередки и другие ситуации, когда при анализе сформированной системы юридических тождеств кроме информационных пробелов следователю приходится констатировать, что некоторые данные не вписываются ни в одно из них. Как правило, это означает ошибочный выбор преступления для квалификации подозрительного деяния либо наличие еще одного преступления. Особенно трудные ситуации возникают при использовании преступниками криптовалют различного вида [Янковский Р.М., 2020: 43–77].

Приходится признать, что использование информации вероятностного характера и в уголовном, и в уголовно-процессуальном праве допускается лишь в качестве ориентирующей, а при обосновании решения о возбуждении уголовного дела следователю приходится понимать риски, связанные с недостаточностью имеющихся данных о проверяемом деянии. Поэтому для обоснования принимаемого решения следователю необходимо использовать профессиональные знания не только в сфере уголовного и уголовно-процессуального права, но и криминалистики [Шмонин А.В., 2017: 73–77]. Именно в криминалистике развиты вероятностные подходы в рамках версионного мышления следователя.

Детальный анализ содержательных особенностей информационных пробелов в сформированной системе юридических тождеств позволяет выдвинуть не только обоснованные следственные версии, нацеленные на поиск способов заполнения информационных пробелов на стадии возбуждения уголовного дела. На их основе возмож-

но спланировать план первоочередных следственных действий сразу же после возбуждения уголовного дела. Фактически речь может идти об оценке следователем рисков совершения юридических ошибок, как это принято в риск-менеджменте [Лузгин И.М., 1981: 115–134]. В рамках его различных схем обычно рекомендуется вначале формализовать возникающие риски, затем разработать организационные и иные меры по их снижению, а для оставшихся «неснижаемых» рисков применяются определенные способы их покрытия.

Разрешение подобных ситуаций имеет еще больше общих признаков с действиями по риск-менеджменту. Следователь понимает, что на основе совокупности данных, достаточность которых он установил по результатам их сопоставления с признаками состава преступления при обосновании решения о возбуждении уголовного дела, он сможет на первоначальном этапе его расследования получить необходимые доказательства. Таким образом, он формализует риски совершения юридических ошибок на основе не только уже проанализированных им данных, но и с использованием навыков версионного мышления. Для покрытия рисков возможных юридических ошибок у него имеется достаточно возможностей для выполнения дополнительных следственных действий, нацеленных на получение необходимых доказательств.

Вместе с тем анализ положений ст. 215 УПК показывает, что содержательные особенности использованного в данной статье критерия достаточности собранной совокупности доказательств существенно отличаются от использованного в ст. 171 УПК. Поэтому риски совершения юридических ошибок, связанные с обоснованием предъявления обвинения определенному лицу, могут покрываться при дальнейшем расследовании уголовного дела.

Раскрытие критерия достаточности собранной совокупности доказательств, использованного в ст. 215 УПК, может осуществляться на основе юридических алгоритмов, в состав которых имплементирована двойная система юридических тождеств [Новиков А.М., 2022: 82–83]. В левой части каждого юридического тождества первой их системы приведено описание обстоятельств, подлежащих доказыванию по расследуемому уголовному делу, которые перечислены в ст. 73 УПК, а в правой — содержание сведений в полученных доказательствах, прошедших надлежащую проверку и оценку. В левой части каждого из юридических тождеств второй системы приведено описание каждого из признаков состава данного преступления, а в правой — содержание сведений по соответствующим доказательствам.

По результатам анализа содержательных особенностей информационных пробелов в сформированной таким образом двойной системе юридических тождеств следователь получает возможность сформировать дополнительный, проблемно-ориентированный план расследования уголовного дела, нацеленный на получение недостающих доказательств. Если и после его выполнения информационные пробелы устранить не удается, то это может стать основанием для принятия решений, предусмотренных ст. 24 УПК в связи с отсутствием состава преступления.

Если же в двойной системе юридических тождеств по киберпреступлению в сфере экономики остаются «лишние» доказательства, не соответствующие признакам его состава, то необходима проверка соответствия собранной совокупности доказательств «смежному» киберпреступлению данного вида, а также о возможном наличии второго преступления, т.е. о совершении совокупности преступлений рассматриваемого вида.

4. Процессуальная регламентация получения доказательств на основе электронных документов и юридических алгоритмов

Большинство транзакций при совершении киберпреступлений в сфере экономики осуществляется с широким использованием компьютерной техники и информационных технологий [Савенко Н.Е., 2023: 145–171]. При этом важно понимать содержательные особенности правовых новелл, введенных в последние годы, и прежде всего обязательственных прав нового вида — цифровых прав. Тем более что на их основе введены цифровые финансовые активы и цифровой рубль, создается система международных взаиморасчетов с использованием национальных валют и т.п.

Что касается важнейших особенностей этого вида обязательственных прав, то законодатель ввел новое понятие «правил информационной системы», которые законодательно пока не урегулированы и устанавливаются самими обладателями информационных систем. При выявлении следов преступлений рассматриваемого вида в электронных документах различных субъектов приходится понимать не только особенности правил этих информационных систем, но и особенности использованного программного обеспечения. Кроме того, при разработке соответствующих систем юридических алгоритмов и основанных на их применении информационных технологий следует обеспечить возможности обработки электронной информации из

«цепочек» информационных систем, с помощью которых осуществлялись регистрация, хранение, передача, преобразование и контроль над накоплением возможных искажений документированной электронной информации.

В созданные на основе юридических алгоритмов обработки электронных документов интерактивные информационные системы могут быть имплементированы информационные эталоны различного вида и назначения. В первую очередь к ним можно отнести ориентированные на выявление и фиксацию в документированной электронной информации данных, могущих стать поводом принятия решения следователем о возбуждении уголовного дела либо об отказе в его возбуждении, а затем и на установление их достаточности. Такие интерактивные информационные системы могут создаваться для их применения в многопользовательском режиме. Это обеспечивает взаимодействие следователя с оперативными сотрудниками при обработке электронной информации, имеющей значение для уголовного дела, в режиме реального времени.

Особого внимания требует разработка научных, правовых и информационно-технологических основ для оперативного выявления признаков приготовления и покушения на совершение тяжких и особо тяжких киберпреступлений в сфере цифровой экономики. Для этого могут быть сформированы информационные эталоны на основе информационных технологий формирования развернутых уголовно-правовых характеристик преступлений данного вида в их динамике, начиная с формирования замысла организатора преступления и осуществления приготовления к их совершению.

Не менее важную роль в создании интерактивных информационных систем данного вида могут сыграть юридические алгоритмы и информационные эталоны, нацеленные на информационно-технологическое обеспечение надлежащей реализации положений ст. 144 УПК, регламентирующих получение дополнительных данных о проверяемом деянии. Эта группа юридических алгоритмов может использоваться многократно, если в соответствующих системах юридических тождеств возникают информационные пробелы. Такой режим их использования позволяет минимизировать риски юридических ошибок при обосновании решения о возбуждении уголовного дела. Аналогичный вывод следует и в отношении случаев, когда при анализе системы юридических тождеств выявляются «лишние» данные, не соответствующие признакам состава преступления, из-за чего возникают информационные неопределенности, создающие риски юридических ошибок.

В сложившейся системе использования разнотипной электронной документации, в которой отражаются особенности выполняемых транзакций субъектами цифровых прав по киберпреступлениям в сфере экономики уже при выполнении неотложных мер следователь сталкивается с проблемами, связанными с отсутствием процессуальной регламентации использования электронных документов в рамках досудебного производства.

Аналогичный вывод следует и в отношении процессуальной регламентации использования в уголовном судопроизводстве тех компьютерных программ, которые применяются брокерами, трейдерами, клиринговыми центрами и другими участниками биржевых транзакций в их информационных системах, в том числе для защиты сведений об осуществленных ими операций от несанкционированного доступа третьих лиц с целью манипулирования рынком и использования инсайдерской информации [Ефимова Л.Г., 2020: 114–120]. Поэтому даже «продвинутые» специалисты и эксперты в сфере разнообразных компьютерных программ далеко не всегда могут оказать необходимую помощь следствию.

Важно также, что если в локальных компьютерных сетях отечественные компьютерные программы, которые могут быть сертифицированы и для применения в уголовном судопроизводстве, вполне конкурентоспособны, то Интернет находится под полным контролем наших западных «партнеров». Кроме того, для финансовых взаиморасчетов стран БРИКС создается специальная информационно-сетевая инфраструктура, в том числе с использованием не только отечественного программного обеспечения, но и иностранных программ, обеспечивающих обмен соответствующими цифровыми финансовыми активами [Тимошенко А.А., 2023: 21–30].

Анализ перечисленных, а также ряда других особенностей программно-аппаратного обеспечения, используемого для создания информационно-телекоммуникационной инфраструктуры государства, показывает, что переход на отечественное программное обеспечение во всех сферах российской экономики и финансов займет весьма длительное время. Поэтому кроме создания отечественного программного обеспечения на основе описанных выше юридических алгоритмов для уголовно-правовой защиты субъектов современной экономики необходима разработка научных и информационно-технологических основ системы сертификации любого программного обеспечения для его использования в уголовном судопроизводстве.

Таким образом, на основе детального описания иерархических систем юридических алгоритмов возможна организация инфор-

мационной поддержки расследования киберпреступлений в сфере экономики с использованием криминалистических и экспертных методик нового типа. Многие из таких методик могут быть реализованы с использованием проблемно-ориентированного программного обеспечения, имплементированного в состав интерактивных информационных систем.

Необходимо обратить внимание и на то, что некоторые из преступлений рассматриваемого вида могут совершаться только для маскировки основного преступления, для чего оставляются их явные, легко выявляемые следы, а сами такие преступления значительно проще в расследовании [Бычков В.В., 2022: 166–173]. В то же время следы основного преступления тщательно маскируются, электронная информация кодируется с помощью оригинального программного обеспечения, а также применяются иные высокотехнологичные способы противодействия их расследованию.

Для таких совокупностей киберпреступлений особую роль приобретает разработка научных основ «динамического», многоэтапного формирования предмета доказывания по соответствующим уголовным делам и дискретизации процедур установления пределов доказывания по каждому из них. Поэтому необходимо в процессе расследования уголовного дела уделять преимущественное внимание тем «лишним» доказательствам и информации, имеющей значение для уголовного дела, которые не полностью соответствуют обязательным и факультативным признакам состава данного преступления.

С помощью интерактивных информационных систем выполняется формирование предмета доказывания для двух преступлений — первоначально расследованного и еще одного, состав которого имеет признаки, совпадающие с «лишними» доказательствами. После этого выполняется новый цикл следственных действий, включая формирования дополнительного плана расследования первоначально возбужденного уголовного дела.

На том этапе, когда с использованием сформированной на основе собранной заново совокупности доказательств будут сформированы две двойных системы юридических тождеств, позволяющих установить наличие двух составов преступления, следователь получает возможность принять решение о выделении и принятии выделенного дела или материалов дела к своему производству. Получив новые доказательства, после анализа сформированных двойных систем юридических тождеств следователь вновь получает несколько возможностей дальнейших процессуально регламентированных действий.

Прежде всего он имеет возможность соединить уголовные дела на новом витке своего понимания их важнейших особенностей, принимая решение в соответствии с положениями ст. 153 УПК, и после этого проводить расследование данного уголовного дела в установленном порядке. Кроме того, речь идет и об иных ситуациях, когда уголовные дела были возбуждены в отношении нескольких лиц, совершивших одно или несколько преступлений в соучастии.

Таким образом, использование проблемно-ориентированных интерактивных информационных систем для обработки электронных документов позволяет надлежащим образом сформировать предмет доказывания по киберпреступлениям в сфере экономики, а также создать научные основы применения нового инструментария при получении доказательств и доказывании по соответствующим уголовным делам.

Заключение

Сложившиеся в уголовно-процессуальном правоприменении методы идентификации предмета доказывания по уголовным делам применительно к киберпреступлениям в сфере цифровой экономики нуждаются в существенной модернизации. Аномально высокий уровень латентности по многим видам киберпреступлений отражает появление ряда новых проблем в борьбе с криминалом, существенно осложняющих переход к информационному обществу и экономике знаний.

Соответственно перед всей системой российского уголовного судопроизводства и правоохранительными органами встают задачи формирования научно обоснованного и выверенного с правовой точки зрения информационно-технологического инструментария для защиты от высокотехнологичного криминала.

Среди наиболее актуальных задач выделяются следующие.

Разработка научно обоснованных изменений и дополнений уголовно-процессуального законодательства, регламентирующих применение определенного программного обеспечения при выполнении следственных действий по получению, проверке и оценке доказательств на основе результатов обработки электронных документов и иной электронной информации, имеющей значение для уголовного дела.

Разработка необходимых правовых норм, регламентирующих требования к правилам информационных систем, устанавливаемых их обладателями, и предусматривающих виды ответственности за их нарушение.

Процессуальная регламентация применения юридических алгоритмов, простых и двойных систем юридических тождеств, а также системы информационных эталонов различного вида и назначения, позволяющих создать проблемно-ориентированное программное обеспечение и интерактивные информационные системы для получения, проверки и оценки доказательств по уголовным делам о киберпреступлениях различного вида.

Процессуальная регламентация применения интерактивных информационных систем для оперативного контроля потоков информации в режиме реального времени, позволяющих выявлять и фиксировать признаки уголовно наказуемых приготовлений к совершению тяжких и особо тяжких киберпреступлений.

Процессуальная регламентация применения юридических алгоритмов и соответствующих проблемно-ориентированных интерактивных информационных систем для создания на их основе государственной системы сертификации отечественного и иностранного прикладного и системного программного обеспечения для его применения при получении, проверке и оценки доказательств по уголовным делам на основе электронных документов и иной электронной информации.

Решение данных задач требует серьезных организационных усилий, материального и кадрового обеспечения. Аналогичный вывод можно сделать и в отношении разработок, нацеленных на создание необходимого комплекса прикладного программного обеспечения на основе систем юридических алгоритмов, информационных эталонов и систем юридических тождеств. Соответствующие проблемы обсуждаются в наших других работах.

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. Бастрыкин А.И. (ред.) Информационные технологии в уголовно-правовой сфере. М.: ЮНИТИ-ДАНА, 2023. 279 с.

3. Бастрыкин А.И. (ред.) Организация и методика расследования отдельных видов экономических преступлений. М.: Спутник+, 2016. 624 с.

4. Бычков В.В. Концептуальная, стратегическая и доктринальная основа законодательного противодействия в Российской Федерации преступлениям экстремистской направленности, совершенным с использованием информационно-телекоммуникационных сетей // Ius Publicum et Privatum, 2022. № 1. С. 166–173.

5. Володина Л.М. Уголовный процесс: проблемы правового регулирования досудебного производства // Право. Журнал Высшей школы экономики. 2024. Том 17. № 2. С. 195–214.

6. Волынский А.Ф. Криминалистика и криминалистическая деятельность. М.: ЮНИТИ-ДАНА, 2019. 440 с.

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

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

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

10. Дикарев И.С. Модернизация системы досудебного производства в уголовном процессе // Legal Concept–Правовая парадигма. 2017. № 2. С. 117–122.

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

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

13. Лузгин И.М. Моделирование при расследовании преступлений. М.: Юридическая литература, 1981. 152 с.

14. Новиков А.М. Доказательства и доказывание в следственной практике. М.: Московская академия Следственного комитета России, 2022. 184 с.

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

16. 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.

17. Соя-Серко Л.А. Программирование расследования // Социалистическая законность. 1980. № 1. С. 33–34.

18. Стойко Н.Г. Возбуждение уголовного дела: замысел законодателя и его реализация // Библиотека криминалиста. 2014. № 1. С. 168–173.

19. Талапина Э.В. Обработка данных при помощи искусственного интеллекта и риски дискриминации // Право. Журнал Высшей школы экономики. 2022. Том 15. № 1. С. 4–27.

20. 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.

21. Тимошенко А.А. Пределы свободной оценки доказательств по уголовным делам // Российский журнал правовых исследований. 2016. № 3. С. 114–120.

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

23. Янковский Р.М. Криптовалюты в российском праве: суррогаты, «иное имущество» и цифровые деньги / Право. Журнал Высшей школы экономики. 2020. Том 13. № 4. С. 43–77.

References

1. Abdulvadiev A.F. et al. (2021) Crimes committed with the use of information technologies: problems of qualification and features of the investigation. Tyumen: University Press, 376 p. (in Russ.)

2. Bastrykin A.I. (ed.) (2023) Information technologies in the criminal law sphere. Moscow: UNITY-DANA, 279 p. (in Russ.)

3. Bastrykin A.I. (ed.) Organization and methodology of investigation of certain types of economic crimes. Moscow: Sputnik+, 2016. 624 p. (in Russ.)

4. Bychkov V.V. (2022) Conceptual, strategic and doctrinal basis for legislative counteraction in the Russian Federation to extremist crimes committed using information and telecommunication networks. Ius Publicum et Privatum, no. 1, pp. 166–173 (in Russ.)

5. Dikarev I.S. (2017) Modernization of the pre-trial proceedings system in criminal process. *Legal Concept–Legal Paradigm*, no. 2, pp. 117–122 (in Russ.)

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

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

8. Golovko L.V. (ed.) (2016) Course of criminal procedure. Moscow: Statut, 657 p. (in Russ.)

9. Luzgin I.M. (1981) *Modeling in the investigation.* Moscow: Juriducheskaya literatura, 152 p. (in Russ.)

10. Novikov A.M. (2022) Evidence and proof in investigative practice. Moscow: Moscow Academy of the Investigative Committee of Russia, 184 p. (in Russ.)

11. Opalsky A.P. (ed.) (2022) Lessons from law enforcement practice in the fight against market manipulation: manual. Moscow: Alpen-Print, 100 p. (in Russ.)

12. 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.)

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

14. Soya-Serko L.A. (1980) Investigation programming. *Sotcialisticheckaya zakonnost*=Socialist Legality, no. 1, pp. 33–34 (in Russ.)

15. Stoiko N.G. (2014) Initiation of a criminal case: the legislator's intent and its implementation. *Biblioteka criminalista*=Criminologist's Library, no. 1, pp. 168–173 (in Russ.)

16. Talapina 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.)

17. Timoshenko A.A. (2016) Limits of free assessment of evidence in criminal cases. *Rossiyskiy zhurnal pravovyh issledovaniy*=Russian Journal of Legal Research, no. 3, pp. 114–120 (in Russ.)

18. Timoshenko A.A., Feyzov V.R., Chernov I.V. (2023) Scenario approach to the study of directions of regulation of the cryptocurrency sphere in the Russian Federa-

tion. *Rossiyskiy zhurnal pravovyh issltdovaniy*=Russian Journal of Legal Research, no. 2, pp. 21–30 (in Russ.)

19. Volodina L.M. (2024) Legal regulation of criminal pre-trial procedures. *Pravo. Journal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, vol. 17, no. 2, pp. 195–214 (in Russ.)

20. Volynsky A.F. (2019) *Forensic science and forensic activity.* Moscow: UNITY-DANA, 440 p. (in Russ.)

21. Volynsky A.F. (2020) *Computer forensics in the system of criminal legal protection of the "traditional" and digital economy.* Moscow: Economika, 476 p. (in Russ.)

22. Yankovsky R.M. (2020) Cryptocurrencies in the Russian law: surrogates, "other property" and digital money. *Pravo. Zhurnal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, vol. 13, no. 4, pp. 43–77 (in Russ.)

23. Zhdanov Yu.N., Ovchinsky V.S. (2020) *Cyberpolice of the 21st century. International experience.* Moscow: Miezhdunarodnye otnoshenia, 288 p. (in Russ.)

Информация об авторах:

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

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

Information about the authors:

V.A. Prorvich — Doctor of Law, Doctor of Technical Sciences, Professor.

S.V. Rastoropov — Doctor of Law, Professor.

Статья поступила в редакцию 15.02.2025; одобрена после рецензирования 21.04.2025; принята к публикации 12.05.2025.

The article was submitted to editorial office 15.02.2025; approved after reviewing 21.04.2025; accepted for publication 12.05.2025.