INTERNATIONAL JOURNAL OF RECENTLY SCIENTIFIC RESEARCHER'S THEORY
International scientific journal
ISSN: 2992-8885
VOLUME: 3 ISSUE: 1

ЦИФРОВЫЕ ДОКАЗАТЕЛЬСТВА: ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ ВОПРОСЫ

Хамидов Бахтиёржон Хамидович
Зам заведующий кафедрой Криминалистики и судебной экспертизы Ташкентского государственного юридического университета, доктор философии по юридическим наукам (PhD)
E-mail: Bahtiyor1984bsj@mail.ru
Тел: +99 8 (99) 522-56-54

Третьяков Григорий Михайлович
Доцент кафедры Уголовного процесса и криминалистики ГрГУ им. Я. Купалы, кандидат юридических наук

Аннотация. *В статье анализируется цифровых доказательств с научной и практической точки зрения. В частности, были изучены понятие цифровых доказательств, вопросы, связанные с их сбором, хранением, проверкой, транспортировкой и оценкой. Вместе с тем, критически рассмотрены проблемы и пробелы в практике национального законодательства и правоприменения в области цифровой обработки доказательств. Разработаны научно обоснованные пути и критерии их устранения.*

Статья подготовлена на основе научно-практических исследований и мнений ученых-теоретиков и сотрудников-практиков в области работы с цифровыми доказательствами, а также технических исследований.

В результате проведенного исследования были проанализированы методологические правила работы с цифровыми доказательствами. На основе заключений автора изучены и обоснованы национальное законодательство, следственная и судебная практика, международный опыт и практика, их достижения и недостатки.

Исходя из этого, были разработаны наиболее оптимальные критерии для правоприменяющих субъектов по сбору, проверке и оценке цифровых доказательств.

В статье проанализированы проблемы в данной области с системной, правовой и научно-методической точек зрения, в этой связи даны авторские выводы. Вместе с тем, также освещены вопросы, связанные с обеспечением допустимости цифровых доказательств, их проверкой и оценкой экспертных заключений. Разработаны научно обоснованные предложения и рекомендации для законодателя и правоприменителя.

Ключевые слова: *электронное доказательство, цифровое доказательство, идентификация, аутентификация, имейдж, хэш-функция.*

ВВЕДЕНИЕ

Развитие цифровых технологий создает проблемы, связанные с внедрением новых понятий и терминов в теорию и практику. В частности, если в 90-х годах прошлого века широко использовались такие термины, как "компьютерное доказательство" или "интернет-доказательство", то сегодня понятия "электронное доказательство" или "цифровое доказательство" и

вопросы, связанные с определением их правового статуса, вызывают жаркие споры среди ученых-правоведов.

Эти понятия и термины также широко используются законодательным субъектом при подготовке и принятии различных нормативно-правовых актов. В частности, во многих законах и подзаконных актах, принимаемых нашим правительством, можно встретить такие термины, как "Цифровой Узбекистан", "цифровая экономика", "цифровая маркировка" или "электронная цифровая подпись", "электронные государственные услуги", "электронные данные", "электронная покупка" или "электронная платформа".

К сожалению, в этом отношении в законодательстве отсутствуют монографические исследования, подтверждающие, какой именно термин является научно правильным и обоснованным. В этом смысле определение правового статуса терминов, относящихся к цифровым технологиям, и разработка научно-теоретических правил можно считать одной из системных проблем в теории и практике права.

По сути, любому термину целесообразно придать юридический статус после его полного научного обоснования. В связи с этим теория, в отличие от законотворчества, исследует различные взгляды и понятия и дает научно обоснованные выводы. Однако такая возможность не всегда доступна при подготовке и принятии нормативно-правовых актов. Поэтому естественно, что для поиска оптимального решения проблемы необходимы определенные научные исследования.

Общетеоретические взгляды на цифровые доказательства

Среди ученых-юристов и практиков существуют различные взгляды на определение в законодательстве понятия "цифровое" или "электронное" доказательство. Например, ***ученые первой группы*** понятие "электронные доказательства" [1, с. 38; 2, с. 74; 3, с. 40; 4, с. 253; 5, 74-b.] считают правильным. В частности, ученый-правовед О.Ш. Пирматов выдвигает понятие: "электронное доказательство - это информация, содержащая сведения об обстоятельствах, имеющих значение для гражданского судопроизводства, созданная, обрабатываемая, хранимая с использованием технических средств и информационных систем, а также информационных технологий и имеющая другие реквизиты, позволяющие ее идентифицировать".

В то же время ученый обратил внимание на понятие цифровых доказательств. По его мнению, цифровые доказательства - это любые фактические данные, служащие основанием для определения судом наличия

или отсутствия в экономическом процессуальном праве обстоятельств, обосновывающих требования и возражения сторон, и другие обстоятельства, имеющие значение для правильного разрешения экономического дела, а также доказательства, созданные на основе двоичной системы счисления [6, 38-39-с.].

Ученый считает, что понятие электронного доказательства шире, чем цифровых доказательств. Однако в определениях, данных О.Ш. Пирматовым, юридическая природа, сущность и отличительные особенности электронных и цифровых доказательств полностью не раскрыты. Кроме того, в определениях отсутствуют положения, касающиеся обеспечения целостности электронных и цифровых доказательств. Поэтому эти определения нельзя считать исчерпывающими.

По мнению А.Н. Балашова, И.Н. Балашовой, Д.В. Бахтеева, К.Л. Брановицкого, В.В. Долганичева, В.Б. Вехова, В.Н. Григорьева, А.И. Зазулина, О.А. Зайцева, С.В. Зуева, О.А. Максимова, М.О. Медведевой, О.В. Овчинниковой, Д.В. Овсянникова, П.С. Пастухова и О.В. Тушкановой, электронное доказательство - это информация, хранящаяся в любой электронной форме, которая может быть использована в качестве доказательства в судебном процессе. Такие виды доказательств могут быть в виде документов в любой электронной форме, электронных писем или других файлов, а также электронных данных, хранящихся сетевыми или интернет-провайдерами [7, с.253-254]. Эти ученые признали электронные доказательства одним из видов вещественных доказательств. Однако, поскольку понятие "электрон" в определении не имеет достаточной научной обоснованности, оно было использовано неуместно.

Некоторые ученые выразили негативное отношение к определению цифровых доказательств в качестве самостоятельного вида доказательств в уголовном процессе. В частности, Р. И. Оконенко в своем исследовании выдвигает понятие электронного доказательства. По его мнению, сейчас преждевременно говорить о понятии "электронные доказательства" как о категории позитивного права. Поэтому электронное доказательство не является отдельным видом доказательства [8, с. 3].

Аналогичная мысль прослеживается и в исследованиях П.С. Пастухова. Ученый считает, что в Уголовно-процессуальный кодекс Российской Федерации не обязательно вводить новый вид доказательства (электронное доказательство) или новый источник (электронный носитель информации), достаточно уточнить понятие "доказательство". По его мнению, данные

существуют в электронном виде, но они являются одним из видов традиционных доказательств [9].

Если мнение Р. И. Оконенко и П. С. Пастухова считается правильным, то, согласно процессуальному законодательству, критерии сбора, хранения, проверки и оценки этих доказательств (как и вещественных или письменных) должны быть одинаковыми. Однако цифровые доказательства не соответствуют традиционным доказательствам ни по одному из критериев. Поэтому и эти мнения не нашли своего подтверждения на практике.

Ученые второй группы выдвигают понятие "цифровое доказательство" [10, с. 1153; 11]. Сторонниками этой группы являются Б.З.Каримов, Д.М.Топилдиева, А.Ю.Черданцев, Шон Гудисон, Роберт Дэвис, Брайан Джексон, Ричард Сеферштейн, Йоган Кесей, Андре Арнес и другие.

По мнению Шона Гудисона, Роберта Дэвиса и Брайана, цифровые доказательства - это информация, направленная на выявление причинно-следственных связей между людьми и событиями во времени и среде. Эти доказательства носят масштабный характер и требуют особой подготовки и средств по отношению к конкретным действенным, мобильным и материальным доказательствам [12]. Это определение носит общий характер и может быть применено и к традиционным видам доказательств. Поэтому можно считать, что в нем недостаточно отражены особенности, присущие цифровым доказательствам.

Ричард Сеферштейн определяет цифровые доказательства как информацию, хранящуюся через систему счисления "1" и "0" и извлекаемую посредством инструкций, установленных в программе или коде. По его мнению, с помощью этих инструкций можно создавать и хранить любую информацию в виде фото, текста или электронной таблицы. Поиск и использование доказательств, сохраненных таким способом, является растущей областью судебной экспертизы. Эта область постоянно меняется с развитием технологий [13].

Это определение не охватывает характеристики приемлемости и целостности цифровых доказательств. В то же время определение носит практический характер. Однако в теории форма цифровых доказательств состоит не только из системы счисления "1" и "0".

Йоган Кесей (Eoghan Casey) считает, что цифровые доказательства или электронные доказательства - это любая доказательственная информация, хранящаяся или передаваемая в цифровом виде, которая может быть

использована сторонами судебного процесса в судебном разбирательстве [14]. По его мнению, перед принятием цифрового доказательства суд должен определить его релевантность (прямую связь), допустимость и возможность принятия представленной копии или необходимость оригинала [15, с. 567].

Андре Арнес определяет цифровые доказательства как любую цифровую информацию, содержащую достоверную информацию, подтверждающую или опровергающую гипотезу о событии или преступлении [16, 7-b; 17, 152-б].

В определениях, данных Йоганом Кесей и Андре Арнесом, не отражены вопросы, связанные с обеспечением целостности цифровых доказательств (хеш-значений). Поэтому в этих определениях также есть недостатки.

А.Ю. Черданцев в своих исследованиях выдвинул понятие цифрового (электронного) доказательства. По его мнению, цифровые (электронные) доказательства - это информация, хранящаяся или передаваемая в двоичной форме об обстоятельствах, подлежащих выяснению по уголовному делу в процессе сбора, проверки и оценки доказательств [18, с.57]. На наш взгляд, предложенный ученым термин "цифровое (электронное) доказательство" не соответствует техническим характеристикам данного ему определения. При этом в определении не отражены особенности и отличительные признаки электронного доказательства. Кроме того, ограничение понятия цифровых доказательств только уголовно-правовыми сферами подтверждает, что оно разработано в узких рамках. Причина в том, что понятие цифровых доказательств имеет одинаковое содержание и форму для всех отраслей процессуального права.

Определение понятия "цифровое доказательство", данное исследователем Б. Каримовым, довольно близко к истине. По его мнению, цифровое доказательство - это информация, хранящаяся в цифровом устройстве и сети или передаваемая через них, значимая и ценная для работы, возникающая в результате человеческого фактора или киберпроцесса [19, с.172].

Правовой механизм обеспечения целостности цифровых доказательств не определен в уголовно-процессуальном законодательстве России и стран СНГ. В связи с этим целесообразно обратить внимание на передовые зарубежные практики, такие как NIST (2006), NIJ (2001) США, ASPO (2011), Interpol (2019), DFRWS (2008) Великобритании, а также международные стандарты ISO/IEC. При этом установлен правовой статус цифровых доказательств и международно признанные методические критерии работы с ними [20, с. 63].

В частности, Национальный институт стандартов и технологий США (National Institute of Standards and Technology) цитирует определение Йогана Кесей о понятии цифрового доказательства [21, с. 1].

Национальный институт юстиции США (National Institute of Justice - NIJ) формулировал отдельное определение понятиям цифровых доказательств и электронных доказательств. Согласно ему, цифровое доказательство - это информация, хранящаяся или передаваемая в двоичной форме, которая может быть использована в суде [22, с. 38]. Электронные доказательства - это ценная информация и данные для расследования, хранящиеся или передаваемые на электронном устройстве [23, с.49].

В Руководящих указаниях международной организации Интерпол для цифровых криминалистических лабораторий (Global guidelines for digital forensics laboratories) отражены вопросы, связанные с характером электронных доказательств и их экспертизой.

Ассоциация старших офицеров полиции Великобритании (далее именуемая АСОП) разработала несколько методических рекомендаций по работе с цифровыми доказательствами. В частности, в "Лучшем практическом руководстве по электронным доказательствам в компьютерной базе данных" АСОП (версия 4) использовалось понятие "компьютерное электронное доказательство". Согласно ему, компьютерное электронное доказательство - это информация и данные, хранящиеся на компьютере или передаваемые через него, имеющие значение для расследования [25, с. 6]. В "Практическом руководстве АСОП по цифровым доказательствам" (5-я версия), хотя и используется понятие цифрового доказательства, оно не определено.

Логически понятие "доказательство" подтверждает тот факт, что конкретное действие или бездействие, имеющее значение для дела, ранее действительно имело место. Например, когда на месте происшествия обнаружены отпечатки пальцев, следователь находит, снимает и фиксирует следы, ранее оставленные преступником, но не создает или не производит сами следы. Это правило также применяется при работе с цифровыми доказательствами. Следователь осуществляет поиск, изъятие и документирование доказательств, ранее оставленных преступником. Поэтому процессы, связанные с "созданием" и "обработкой" цифровой информации, не участвуют в формировании понятия цифрового доказательства.

Соответственно, можно выдвинуть концепцию о том, что цифровое доказательство - это информация, хранящаяся в цифровой форме, имеющая ценность для дела.

Технические характеристики цифровых доказательств

Согласно физическим законам, электрический ток является результатом упорядоченного движения электрических зарядов [26]. Другими словами, электрический ток является формой энергии. Если электрический ток освещает лампу или приводит в движение двигатель машины, логично использовать термин "электролампа" или "электромобиль" для обозначения этих объектов. Причина в том, что электрическая энергия непосредственно влияет на движение света или материи. Однако механизм формирования цифровой информации совершенно отличается от этих процессов. Вместе с тем в природе не существует определенной формы электрической энергии. Поэтому можно считать, что электрический ток или магнитное поле участвуют только в качестве источника (средства) в возникновении цифровых доказательств.

Для дальнейшего обоснования нашего мнения обратимся к источникам записи. Из истории человечества известно, что надписи сначала писались на скалах, затем на коже, бамбуковых палочках, ткани или бумаге. Источники записи письма постоянно менялись на границе времени и пространства. Следовательно, изменения напрямую связаны с обстоятельствами изобретения или возникновения средств записи. Поэтому под письменными источниками подразумеваются не камни, кожа, ткань или бумага, а надписи на них. В заключение, электрический ток или магнитное поле, как и вышеупомянутые источники, является инструментом, характерным для сегодняшнего дня.

Минимальная единица цифровой информации - ***"бит".*** Как правило, команды компьютера работают не с отдельными битами, а с восемью битами одновременно. Восемь систематизированных битов составляют один ***байт,*** большее количество информации - килобайты, мегабайты [27, 53-b] и т.д.

Большинство цифровых устройств приводятся в движение электрическим током. Технически это верно. Однако с точки зрения источников (электрический ток, магнитное поле) наименование информации "электронным" носит относительный характер. На самом деле, источник не обрабатывает информацию напрямую, а создает условия для этого.

Технически любое цифровое устройство имеет процессор. Большинство процессоров получают и обрабатывают информацию в двоичной форме - через числа "0" и "1". В зависимости от характера информации, процессор передает

ISSN: 2992-8885
VOLUME: 3 ISSUE: 1

цифровую информацию непосредственно пользователю (ассемблер) или через определенные компиляторы [28, с.225]. Другими словами, через комбинацию битов, состоящую из чисел "0" и "1" или "0", "1" и "2", процессор кодирует информацию в цифровой форме. После этого эта информация передается на монитор в различных текстовых, фото-, видео-, аудио-, графических или других формах (форматах).

Как организовать работу с цифровыми доказательствами

Процесс работы с цифровыми доказательствами включает этические, процессуальные и методические правила их сбора, проверки, хранения, транспортировки и оценки. Каждый из этих процессов является самостоятельным этапом, при котором соблюдаются определенные правовые и технические требования.

Методические правила работы с цифровыми доказательствами имеют одинаковое обязательное значение для всех отраслей процессуального права. Вместе с тем, данные положения непосредственно связаны с правами и свободами личности. Кроме того, существует необходимость унификации различных практик работы с цифровыми доказательствами, сложившихся в правоприменительной практике. Поэтому целесообразно, чтобы эти правила были утверждены конкретным уполномоченным субъектом и адаптированы к международной практике и стандартам.

Цифровые доказательства чрезвычайно чувствительны и быстро меняются. Поэтому работа с ними требует специальной подготовки. Причина в том, что в результате одной неосторожности существует высокая вероятность повреждения или утраты ценных для расследования цифровых доказательств. Кроме того, правоприменитель должен уметь самостоятельно анализировать цифровые доказательства, чтобы правильно оценить мнение специалиста или заключение эксперта и определить эффективные направления расследования. Отсутствие таких знаний ставит под угрозу или приводит к искажению достоверности цифровых доказательств. Приговор суда, вынесенный по этому поводу, противоречит закону. Соответственно, целесообразно готовить специальных следователей, прокуроров или судей в этой области.

Специальный следователь - лицо, прошедшее переподготовку в области цифровой криминалистики, уполномоченное расследовать уголовное дело. Он осуществляет руководство следственной и оперативной группой по уголовному делу, является полностью ответственным лицом по делу. При этом разрабатывает план расследования, формирует следственно-оперативную

группу по уголовному делу, распределяет обязанности, определяет направления расследования и осуществляет общее руководство расследованием. Постоянно информирует прокурора об уголовном судопроизводстве, обеспечивает последовательность, эффективность и законность следственных действий. Кроме того, осуществляет контроль за законностью оперативно-розыскных мероприятий, обеспечивает приемлемость процессов сбора, хранения, проверки и оценки цифровых доказательств. Вопросы, связанные с транспортировкой цифровых доказательств, также решаются специальным следователем.

Особенность работы с цифровыми доказательствами заключается в том, что собранные доказательства и их копии одновременно направляются эксперту, прокурору, судье и адвокату, рассматривающему дело. Это создает равные возможности для участников процесса. Причина в том, что после того, как числовые доказательства оценены, их невозможно изменить. В противном случае их приемлемость нарушается.

Основным условием работы с цифровыми доказательствами является их получение с участием эксперта, специалиста. Как правило, специалист предупреждает членов группы о возможных проблемах информационной безопасности, предоставляет предварительную и последующую информацию о конфигурации системы и сети, а также помогает документировать ситуации, связанные с работой. Кроме того, оказывает методическую помощь следователю по другим обстоятельствам дела.

После этого эксперт определяет цифровые доказательства, следы и их источники, снимает с них копии на основании технических требований и документирует последовательность действий, выполненных на цифровом устройстве. Кроме того, анализирует, проверяет цифровые доказательства, относящиеся к делу, дает научно обоснованные выводы и пояснения по результатам исследования.

В процессе работы с цифровыми доказательствами важно обеспечить безопасность территории. При этом инспектор профилактики первым прибывает на место происшествия, докладывает следователю о месте происшествия, обеспечивает ограждение его границ и сохранность вещественных доказательств. В то же время, он документирует посетителей места происшествия (определяет цели, задачи и время).

Оперативно-розыскный сотрудник обеспечивает исполнение поручений следователя в соответствии с установленным порядком, строго соблюдает

правила работы с цифровыми доказательствами и осуществляет необходимые оперативно-розыскные мероприятия.

В процессе работы с цифровыми доказательствами важно участие заявителя или потерпевшего. Следователю целесообразно начать дело с их допроса. Это проясняет сложившуюся ситуацию и определяет механизм совершения преступления. В корпоративных условиях заявителем и жертвой могут быть разные лица.

Вместе с тем в процессе работы с цифровыми доказательствами при необходимости будут участвовать суды, специалисты банков.

«Имейдж» цифровых доказательств [29; 30, 38-b] (визуально), оценивается (хэш-функция) и подтверждается. «Имейдж» цифровых доказательств - надежный способ обеспечения их целостности. Метод имейджа (визуальный) считается простым и трудоемким процессом. В этом случае цифровые доказательства визуально копируются (как изображения) и им присваивается ценность с помощью специальных программ. Если эта величина изменится, целостность доказательства также будет нарушена. Причина в том, что невозможно восстановить заданное значение.

Преимущество копирования цифровой информации имейджем заключается в том, что после переноса доказательства на другое устройство исходное устройство может быть возвращено владельцу. Также стоимость цифрового доказательства направляется в суд в установленном порядке. Этот метод также позволяет защитить цифровые доказательства от любых внешних воздействий.

Для раскрытия и проверки информации, полученной путем визуального («имейдж») копирования, необходимы специальные цифровые криминалистические средства. Например, "Magnet Axiom" [31], "Accessdate" [32], "EnCase," "EnCase FIM" "Elcomsoft" [33], " HYPERLINK "http://www.forensicmall.ru/cat/belkasoft/belkasoft-evidence-center-2016" Belkasoft Evidence Center 2020," "Belkasoft Acquisition and Analysis Suite" и т.д. Эти инструменты предназначены для прямой или удаленной работы с цифровыми доказательствами. Файлы, имеющие важное значение, будут получены и отображены с помощью программного обеспечения цифровой судебной экспертизы. Однако содержание и целостность доказательств или файлов и метаданных не будут изменены.

После осмотра цифрового устройства и доказательств составляется протокол в установленном порядке. В протоколе хеш-значение цифровых

ISSN: 2992-8885
VOLUME: 3 ISSUE: 1

доказательств подписывается понятыми. Таким образом, будут решены процессуальные проблемы, связанные с участием понятых. С помощью специальных программ отчеты о цифровой информации приобщаются к следственному делу. В протоколе также указывается, какие технические устройства и программные средства использовались.

После получения цифровые устройства упаковываются в антистетические пакеты в установленном порядке. Упаковывается в защищенном виде от любых механических повреждений и радиоволн, электромагнитных воздействий. В этом случае USB-канал и канал порта цифрового устройства закрываются снаружи и упаковываются. После этого следователь принимает меры по их транспортировке.

Оценки цифровых доказательств Какие критерии существуют?

Научно-исследовательской работе, следственной и судебной практике, проводимой в нашей стране, отсутствуют единые правила оценки цифровых доказательств. Однако в зарубежных странах этот вопрос широко исследован и по нему сформирована научно обоснованная практика. Поэтому наиболее оптимальным решением является восполнение пробелов в теории и практике, предотвращение и устранение ошибок, возникающих в процессуальном законодательстве, следственной и судебной практике, опираясь на передовой зарубежный опыт.

При оценке цифровых доказательств правоприменитель должен сначала проверить соблюдение правовых, технических и этических норм при их сборе, хранении, проверке и транспортировке [34, с. 95-96]. Причина в том, что при работе с цифровыми доказательствами приходится анализировать персональные данные граждан, не имеющих значения для дела. При этом следователь, прокурор, суд, адвокат, эксперт, специалист и другие участники обязаны обеспечить неразглашение и неприкосновенность этих сведений.

В случаях исследования цифровых доказательств эксперт дает научно обоснованные разъяснения по особенностям, методам и средствам исследования, проведенного в судебном разбирательстве. При этом эксперт (специалист) должен поэтапно задокументировать свои действия, указать методы и средства получения и проверки доказательств, подробно разъяснить критерии оценки и вопросы оценки. Вместе с тем, целесообразно повторное представление результатов исследования эксперта (специалиста) в судебном разбирательстве. Причина в том, что результаты экспертного исследования

должны давать одинаковую ценность при проверке судьей, прокурором и адвокатом.

В ходе исследования была изучена передовая практика многих развитых зарубежных стран, в частности США [35, 498-б], Великобритании [36, 688-б], Австралии [37, 372-б], Норвегии [38, 366], Швеции [39, 227-б] по проверке экспертных показаний и оценке доказательств. Было установлено, что в законодательстве этих стран также установлены строгие требования к экспертным исследованиям, как указано выше.

Оценка доказательств является заключительным этапом их проверки. Поэтому каждое доказательство по делу должно оцениваться отдельно и по совокупности доказательств.

В теории существует ряд мнений и соображений относительно критериев оценки доказательств. В частности, ученые первой группы приняли их достоверность в качестве основного критерия при оценке доказательств. Ученые второй группы считают, что содержание оценки доказательств включает в себя определение всех их характеристик, влияющих на достижение объективной истины по делу [40, с. 150]. Ученые третьей группы при оценке цифровых доказательств учитывают их приемлемость, достоверность, релевантность и значимость.

При оценке доказательств учитываются все особенности цифрового доказательства. Доказательства оцениваются с точки зрения их релевантности, приемлемости, достоверности и достаточности. Однако оценка цифровых доказательств является более сложным процессом, чем материальных доказательств. Это связано с тем, что перед оценкой цифровых доказательств существует ряд требований, которые необходимо соблюдать.

В развитых странах, включая США [41, с. 68-69], установлены предварительные требования к проверке при оценке цифровых доказательств. В частности, В. Руссев предложил следующие основные критерии представления в суд цифровых доказательств или оценки показаний на основе стандарта Доберта [42, с.10].

1. Методы, применяемые в ходе расследования и экспертизы, должны быть теоретически обоснованы. Причина в том, что, согласно действующему законодательству, следственные органы или суд не вправе использовать какие-либо средства и методы для признания лица виновным от имени государства. Эти средства и методы должны быть апробированы в результате конкретных

исследований. В противном случае решение должно быть вынесено в пользу подозреваемого.

2. Методы, используемые в криминалистической практике, должны публиковаться в журналах, газетах или интернет-сайтах правоохранительных органов. При этом другие участники процесса, в том числе судьи и адвокаты, должны быть осведомлены о методологиях, применяемых в следственном и судебном процессе. В противном случае невозможно обеспечить законность и справедливость в суде.

3. Определение степени погрешности метода исследования. При этом проверяется уровень достоверности методов и средств, используемых при проведении исследования.

4. Методы, используемые на практике, должны быть приняты в научном сообществе. Это требование также очень важно, поскольку оно позволяет унифицировать методы, используемые на стадиях досудебного производства и судебного разбирательства.

Эти стандарты предоставляют широкие возможности для проверки точности цифровых доказательств и достоверности экспертных показаний [43, с.45].

В 2017 году Антви-Боасиако (Antwi-Boasiako) и Вентер (Venter) разработали "Единую модель оценки допустимости цифровых доказательств" (Harmonized Model for Digital Evidence Admissibility Assessment (HM - DEAA)) по техническим и правовым требованиям допустимости цифровых доказательств. В этой модели представлены следующие три этапа оценки цифровых доказательств.

а) Оценка допустимости цифровых доказательств

На данном этапе проводится криминалистическая оценка соблюдения процессуального законодательства и международных стандартов при получении цифровых доказательств и их значимости.

б) Рассмотрение цифровых доказательств

На этом этапе оценивается целостность цифровых доказательств, то есть соблюдение процедур и инструментов экспертизы при их получении, хранении и анализе. Целью этого является проверка соблюдения научно обоснованных принципов при обнаружении, хранении и анализе доказательств, обеспечение качества работы и укрепление доверия к результатам [44]. При этом учитывается соблюдение стандартов при работе с цифровыми доказательствами и их исследовании (например, прохождение цифровыми

криминалистическими средствами аттестации, подтверждение их надежности и исправности, апробация перед использованием).

Кроме того, должны быть изучены стандарты и протоколы, применяемые в лабораторных исследованиях. Цель состоит в том, чтобы определить наличие надежных методов, цифровых устройств и программных средств, компетентных сотрудников и возможности делать обоснованные выводы для анализа цифровых доказательств в лаборатории и обеспечения достоверности результатов.

в) Принятие решения о допустимости цифровых доказательств

На этом этапе подлинность, целостность и достоверность цифровых доказательств оцениваются на основе результатов второго этапа. Например, методы и средства получения цифровых доказательств оцениваются с точки зрения их надежности, а показания экспертов сравниваются [45]. Для того чтобы результаты были признаны достоверными, они должны быть объективно истолкованы, а информация об ошибках, неточностях и ограничениях должна быть раскрыта [46, с. 158, 47, с. 95].

Как бы ни были совершенны критерии, предложенные В. Руссевым, Антви-Боасиако и Вентером, в них не указаны этические требования к оценке цифровых доказательств. Следует отметить, что этические требования также имеют принципиальное значение при оценке данного вида доказательств. Действительно, согласно действующему законодательству, личная информация считается конфиденциальной информацией.

В заключение следует отметить, что передовые зарубежные практики и стандарты устанавливают международно признанные правила оценки цифровых доказательств [48, с.15]. Их приведение в соответствие с национальным законодательством будет способствовать положительному решению следующих вопросов:

во-первых, обеспечивается прозрачность правоприменительной деятельности;

во-вторых, внедряется научно обоснованный, объективный, законный и справедливый механизм сбора, хранения, исследования и оценки цифровых доказательств на стадиях досудебного и судебного разбирательства;

в-третьих, в сфере работы с цифровыми доказательствами будут установлены единые методические правила не только для уголовных судов, но и для административных, гражданских и экономических судов;

ISSN: 2992-8885
VOLUME: 3 ISSUE: 1

в-четвертых, позволит обеспечить надежную защиту интересов Республики Узбекистан в спорах, возникающих между государствами в данной сфере.

ЗАКЛЮЧЕНИЕ

В заключение следует отметить, что четкое определение правил работы с цифровыми доказательствами в национальном законодательстве позволяет научно обоснованно решать ошибки и проблемы, возникающие в судебно-правовой сфере, посредством закона. В этом смысле результаты исследования служат методологической основой для унификации различных практик, формирующихся в системе процессуального законодательства.

Кроме того, разработанные теоретические положения обеспечивают решение проблем, связанных с единообразным применением правовой терминологии в процессе подготовки и принятия нормативно-правовых актов.

I. По результатам исследования, законодательный субъект:

- целесообразно использовать понятие "цифровое доказательство" в законотворческой деятельности. Данное понятие полностью соответствует правовым и техническим характеристикам данных доказательств;

Методические правила работы с цифровыми доказательствами являются общими и обязательными для всех отраслей процессуального права (уголовное, гражданское, экономическое процессуальное законодательство и кодекс об административной ответственности). Причина в том, что приемлемость цифровых доказательств обеспечивается не только правовыми требованиями, но и техническими регламентами.

II. В процессе работы с цифровыми доказательствами целесообразно обеспечить следующее правоприменительными субъектами:

- переподготовка субъектов правоприменения (дознавателя, следователя, прокурора и суда) в области цифровой криминалистики (не менее 1 года) (причина в том, что данные субъекты осуществляют правовую оценку обстоятельств, имеющих значение для дела. Непонимание сущности цифровых доказательств и их особенностей препятствует проверке и оценке фактического положения дел);

- приведение правил сбора, хранения, проверки и транспортировки цифровых доказательств в соответствие с передовой зарубежной практикой и международными стандартами (ISO/IEC-27035-1, ISO/IEC-27035-2, ISO/IEC27035-3, ISO/IEC-27037, ISO/IEC-27038, ISO/IEC-27040, ISO/IEC-27041,

ISO/IEC-27042, ISO/IEC-27043 [56], ISO/IEC-27044, ISO/IEC-27050, ISO/IEC-30121);

- утверждение единого для всех государственных органов этического кодекса работы с цифровыми доказательствами; разработка процессуального порядка работы с цифровыми доказательствами. Вместе с тем, внедрение справедливых, законных и эффективных механизмов их аутентификации (проверки подлинности);

- оснащение следственных и судебных органов современными цифровыми криминалистическими средствами и т.д.

III. При оценке цифровых доказательств правоприменитель целесообразно опираться на следующие критерии:

- оформление цифровых доказательств с соблюдением требований процессуального закона;

- применение научно обоснованных методов и средств сбора, хранения, проверки и транспортировки цифровых доказательств;

- обеспечение допустимости цифровых доказательств;

- наличие у эксперта соответствующего квалификационного сертификата по рассматриваемому делу, испытание и аккредитация средств исследования экспертного учреждения в установленном порядке.

Эти критерии полностью соответствуют национальным и международным стандартам оценки цифровых доказательств и служат установлению справедливости на стадиях досудебного производства и судебного разбирательства.

Список литературы:

1. Пирматов О.Ш. Процессуальные аспекты электронных доказательств в экономическом и гражданском судопроизводстве. диссертация доктора философии (PhD) по юридическим наукам. 2020 г. С. 1-155.
2. Кадирова М.К., Абдуллаев Р.К., Хужаназаров А.А., Рахимкулова Л.У. Оценка результатов судебных компьютерных и технических экспертиз следователями и судом. 2020. 74 С. DOI: 10.37200/IJPR/V24I6/PR260256. Hyperlink "https://www.psychosocial.com/article/PR260256/13667/" https://www.psychosocial.com/article/PR260256/13667/
3. Вехов В. Б. Электронная криминалистика: понятие и система //Криминалистика: актуальные вопросы теории и практики: сб. трудов участников международно-науч.-практич. конф. - Ташкент, 2017. 44-60.

4. Зуев С.В. Основы теории электронных доказательств: монография / под ред. д. юрид. наук С.В. Зуева. М., 2019. С. 253-270.
5. Абдуллаев Р.К. Широкое использование электронных технологий в уголовном судопроизводстве. Журнал юридических исследований. 2020, том 2, выпуск 5, стр. 1-255.
6. Пирматов О.Ш. Процессуальные аспекты электронных доказательств в экономическом и гражданском судопроизводстве // Диссертация доктора философии (PhD) по юридическим наукам - Т.; ТГЮУ. 2020 г. 38 С. Там же 38 - 39 С.
7. Основы теории электронных доказательств: монография / под ред. д. юрид. наук С.В. Зуева. - Ташкент, 2020. С. 253, 254.
8. Оконенко Р.И. "Электронные доказательства" и проблемы обеспечения прав граждан на защиту тайны частной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дис.... канд. юрид. наук. М., 2016.
9. Пастухов П. С. О развитии уголовно-процессуального доказывания с использованием электронных доказательств // СПС "КонсультантПлюс".
10. Хамидов Б.Х., Каримов Б.З., Топилдиева Д.М. Общие теоретические вопросы совершенствования частных судебно-медицинских методов в области борьбы с киберпреступностью. Психология и образование (2021) 58 (1): 2705-2712. ISSN:00333077/ 2021. https://doi.org/10.17762/pae.v58i1.1153.
11. Jones, Andrew (2008). Создание лаборатории цифровой криминалистики. Баттерворт-Хайнеманн. стр. 312. ISBN 978-1-85617-510-4. Цифровая криминалистика - https://ru.qaz.wiki/wiki/Digital_forensics.
12. Шон Э. Гудисон, Роберт К. Дэвис и Брайан А. Джексон. Цифровые доказательства и система уголовного правосудия США - Выявление технологий и других потребностей для более эффективного получения и использования цифровых доказательств. 2015.
13. Саферштейн, Ричард. Упрощенное руководство по цифровым доказательствам. National Forensic Science Technology Center®NFSTC Largo, Флорида 2015.
14. Casey, Eoghan (2004). Цифровые доказательства и компьютерная преступность, второе издание. Elsevier. ISBN 0-12-163104-4.
15. Various (2009). Eoghan Casey (ред.). Справочник по цифровой криминалистике и расследованию. Academic Press. p. 567. ISBN 978-0-12-374267-4. Получено 2 сентября 2010.

16. Андре Арнес. "Цифровая криминалистика." Хобокен, Норвегия. John Wiley & Sons Ltd. 2018. - 7 с.
17. Каримов Бобуржон (2020). Научно-теоретические вопросы категории цифровых доказательств. Обзор юридических наук, 5 (Специальный выпуск), 149-153. doi: 10.24412/2181-919X-2020-149-153.
18. Хамидов Б.Х., Каримов Б.З. Некоторые вопросы в разработке национальной стратегии кибербезопасности: проблема и анализ. Европа, наука и мы | европа, веда и мы | европа, наука и мы Образование и наука, Чехия. 2020. 63 с.
19. Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang. Руководство по интеграции криминалистических методов в реагирование на инциденты // Рекомендации Национального института стандартов и технологий NIST Специальное издание 800-86. 2006. Э-1, с.
20. U.S. Department of Justice Office of Justice Programs National Institute of Justice. Электронное расследование сцен преступлений: Руководство для первых ответчиков, второе издание. 2001. 38 с.
21. U.S. Department of Justice Office of Justice Programs National Institute of Justice. Электронное расследование сцен преступлений: Руководство для первых ответчиков, второе издание. 2001. 49 с.
22. Черданцев А. Ю. Понятие цифровых доказательств, современное состояние и их роль в доказывательном процессе. Юридическая наука и практика. 2019. Том 15, No 4. С. 55-60. DOI: 10.25205/2542-0410-2019-15-4-55-60.
23. Каримов Б.З. Научно-теоретические вопросы категории цифровых доказательств. Научная статья - Т.: Вестник юридических наук ТГЮУ - Вестник юридических наук - Review of Law Sciences. 5 (2020) 168 с. (168-172 с.).
24. Interpol Global guidelines for digital forensics laboratories. 2019. - С. 13-78.
25. ACPO Good Practice Guide for Computer-Based Electronic Evidence. Официальный релиз версии 4.0. - С. 6-66.
26. https://skachat-besplatno.info/ximfiz/237-doimiy-elektr-toki-va-uning-1179onunlari.html
27. Ионова Ю.А., Калитин С.В. Понятие доказательств, имеющих электронную форму и цифровое содержание: проблемы и перспективы. Статья. Вестник МГАЭП. 2013. No 1 (63) с. 53.
28. Хамидов Бахтиёр. Общетеоретические вопросы совершенствования частных криминалистических методологий в сфере борьбы с

киберпреступностью // Review of law sciences. 2020. No Спецвыпуск. URL: https://cyberleninka.ru/article/n/obscheteoreticheskie-voprosy-sovershenstvovaniya-chastnyh-kriminalisticheskih-metodologiy-v-sfere-borby-s-kiberprestupnostyu (дата обращения: 11.03.2021).

29. SWGDE Best Practices for Image Authentication, 2018; SWGDE Best Practices for Image Content Analysis, 2017; SWGDE Guidelines for Forensic Image Analysis, 2017. https://www.unodc.org/e4j/ru/cybercrime/module-6/key-issues/handling-of-digital-evidence.html
30. Каримов Б.З. Использование возможностей цифровой криминалистики в уголовных делах. Монография. - Т., 2021.- 38 с.
31. http://www.forensicmall.ru/cat/magnet-forensics/magnet-axiom/
32. http://www.forensicmall.ru/cat/category/accessdata/
33. http://www.forensicmall.ru/cat/category/belkasoft/
34. Хамидов Б. Проверка и оценка результатов цифровой экспертизы // Общество и инновации. - 2021. - Т. 2. - No 2. 3. - С. 91-97.
35. Альберт Дж. Марцелла, Младший. Даг Менендес. "Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes." 2-е издание. Нью-Йорк, США. Taylor & Francis Group, LLC. 2008. - 498 с.
36. Anthony T.S. Ho and Shujun Lee. "Справочник по цифровой криминалистике мультимедийных данных и устройств." Гилдфорд, Великобритания. John Wiley & Sons, Ltd. - 688 с.
37. Ричард Боддингтон. "Практическая цифровая криминалистика." Бирмингем, Великобритания. Packt Publishing Ltd. - 372 с.
38. Андре Арнес. "Цифровая криминалистика." Хобокен, Норвегия. John Wiley & Sons Ltd. 2018. - 366 с.
39. Joakim Kävrestad. "Основы цифровой криминалистики." Skövde, Швеция. Springer International Publishing. - 227 с.
40. Фаткуллин Ф.Н. Общая проблема процессуального доказывания. Казань, 1973. С.150.
41. Андре Арнес. Цифровая криминалистика. John Wiley & Sons, Inc., 111 River Street, Hoboken, USA 2018. стр. 68-69.
42. Василь Руссев. Цифровая криминалистическая наука: проблемы, методы и вызовы. Morgan & Claypool Publishers. Университет Техаса, Сан-Антонио. 2016. - С. 10.

43. Goodstein, D. Reference Manual on Scientific Evidence, 3rd ed., National Academies Press, 2011, ch. Допустимость экспертных показаний, стр. 37-54.
44. SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs, 2017.
45. Antwi-Boasiako and Venter, 2017; Национальный институт юстиции США, 2004.
46. Б.Х. Хамидов. Проверка и оценка экспертных показаний при расследовании киберпреступлений. Международная конференция по науке и образованию / Международная конференция по науке и образованию. 2021. http://doi.org/10.37057/T_1 (155-158).
47. Хамидов Б. Проверка и оценка результатов цифровой экспертизы // Общество и инновации. - 2021. - Т. 2. - No 2. 3. - С. 91-97.
48. Хамидов Б. (2021). Общие теоретические вопросы, связанные с цифровыми доказательствами: проблема и решение. Norwegian Journal of Development of the International Science. doi:10.24412/3453-9875-2021-63-2-8-16.
49. Bakhronova, D., Alavutdinova, N., Israilova, S., & Vilchis, V. V. Color Lexemes in Context: Cognitive and Cultural Explorations.
50. https://webstore.iec.ch/preview/info_isoiec27043%7Bed1.0%7Den.pdf