

UDC: 343.2

ПРОИЗВОДСТВО ДОСЛЕДСТВЕННОЙ ПРОВЕРКИ ПО ДЕЛАМ О МОШЕННИЧЕСТВЕ: ТАКТИЧЕСКИЕ ОСОБЕННОСТИ, ПРОБЛЕМЫ И СПОСОБЫ ИХ РЕШЕНИЯ

Сабырбаева Айнура Бахыт кизи,
доктор философии по юридическим наукам (PhD),
преподаватель кафедры «Уголовно-процессуальное право»
Академии МВД Республики Узбекистан
ORCID: 0000-0002-8364-5319
e-mail: ww.a_sabyrbaeva@inbox.ru

Аннотация. Технический прогресс, модернизация предпринимательской деятельности, возникновение новых способов заработка, бизнеса, развитие экономических отношений обусловили повышенный интерес со стороны мошенников. Традиционные виды мошенничества, такие как обещание трудоустройства потерпевшего, не предполагали такую географию преступления и круг потерпевших, как при современных видах мошенничества с использованием информационно-коммуникационных технологий, сети Интернет, программ обеспечения, социальных мессенджеров. В данной статье рассматривается процессуальный порядок производства доследственной проверки по современным видам мошенничества, а также тактические особенности его производства. Для решения трудностей в расследовании современных форм мошенничества, таких как маскировка под гражданско-правовые деликты, разработаны критерии для их отграничения. Также приведен перечень вопросов и обстоятельств, подлежащих установлению при производстве доследственной проверки, а также порядок изъятия, осмотра и оформления новых видов доказательств. Несмотря на компьютеризацию всех сфер общества, появление новых видов совершения мошенничества, выявление новых видов доказательств и следов (электронных), процессуально не урегулирован порядок изъятия, осмотра и оформления электронных доказательств (отсутствует само понятие электронного доказательства), так и нет единого подхода по производству тех или иных следственных действий для обнаружения и изъятия этих доказательств. В статье приведены мнения ученых касательно понятийного аппарата электронного доказательства, а также по тактике производства изъятия, осмотра и фиксации электронных доказательств с использованием современных технологий и программ обеспечения. В заключение выдвинуты предложения по внесению изменений и дополнений в уголовно-процессуальное законодательство.

Ключевые слова: мошенничество, фиксация, электронное доказательство, информационно-коммуникационные технологии, программы обеспечения, доследственная проверка.

FIRIBGARLIK HOLATLARIDA TERGOVGA QADAR TEKSHIRUV: TAKTIK XUSUSIYATLARI, MUAMMOLARI VA UNING YECHIMLARI

Sabirbayeva Aynura Baxit qizi,
O'zbekiston Respublikasi Ichki ishlar vazirligi Akademiyasi
"Jinoyat-protsessual huquqi" kafedrası o'qituvchisi,
yuridik fanlar bo'yicha falsafa doktori (PhD)

Annotatsiya. *Texnik rivojlantirish, tadbirkorlik faoliyatini modernizatsiya qilish, pul topish, biznes qilishning yangi turlari paydo bo'lishi, iqtisodiy munosabatlarning rivojlanishi bu sohaga firibgarlarning qiziqishi kuchayishiga olib kelgan. Firibgarlikning an'anaviy turlari, masalan, jabrlanuvchini ishga joylashtirish bilan aldash orqali pullarini egallab olish kabi firibgarlik jinoyatlari zamonaviy turdagi (Axborot-kommunikatsiya texnologiyalari, Internet tarmog'i, dastur ta'minotlari, ijtimoiy tarmoqlar, to'lov kartalari yordamida sodir etilgan) firibgarlik jinoyatlaridek jabrlanuvchilar doirasini qamrab olmaydi. Ushbu maqolada firibgarlikning zamonaviy turlari bo'yicha tergovga qadar tekshiruv o'tkazishning protsessual tartibi, shuningdek, uni o'tkazishdagi taktik xususiyatlar o'rganilgan. Firibgarlikning zamonaviy shakllarini tergov qilishdagi qiyinchiliklarni hal qilish uchun, masalan, fuqarolik munosabatlari ostida yashiringan firibgarliklarni aniqlash mezonlari ishlab chiqilgan. Maqolada tergovga qadar tekshiruv paytida aniqlanishi lozim bo'lgan masalalar va holatlar ro'yxati, shuningdek, yangi turdagi dalillarni olib qo'yish, ko'zdan kechirish va ro'yxatdan o'tkazish tartibi keltirilgan. Jamiyatning barcha sohalarini kompyuterlashtirishga qaramay, yangi turdagi dalillar va izlarni (elektron) aniqlash, elektron dalillarni olib qo'yish, ko'zdan kechirish va ro'yxatdan o'tkazish tartibi huquqiy tartibga solinmagan ("elektron dalillar" tushunchasi hattoki mavjud emas), shuningdek, bunday dalillarni aniqlash va olib chiqish uchun muayyan tergov harakatlarini o'tkazishda yagona yondashuv yo'q. Maqolada olimlarning "elektron dalillar" konseptual apparati, zamonaviy texnologiyalar va dasturlardan foydalangan holda, elektron dalillarni olib qo'yish, ko'zdan kechirish va rasmiylashtirish taktikasi haqidagi fikrlari keltirilgan. Xulosa qismida jinoyat-protsessual qonunchiligiga o'zgartish va qo'shimchalar kiritish bo'yicha takliflar ilgari surilgan.*

Kalit so'zlar: *firibgarlik, fiksatsiya, elektron dalil, axborot-kommunikatsiya texnologiyalari, dasturiy ta'minot, tergovga qadar tekshiruv.*

PRODUCTION OF PRE-INTERVIEW CHECK IN CASES OF FRAUD: TACTICAL FEATURES, PROBLEMS AND WAYS TO SOLVE THEM

Sabyrbaeva Aynura Bakhyt kizi,

Lecturer of the Department of Criminal Procedure Law
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan,
Doctor of Philosophy in Legal Sciences (PhD)

Abstract. *Technological progress, modernization of entrepreneurial activity, applying new ways of earning, business, the development of economic relations has led to increased interest of fraudsters. Traditional types of fraud, such as the promise of employment of the victim, did not assume such a geography of the crime and the circle of victims, as with modern types of fraud using information and communication technologies, the Internet, software, social messengers. This article discusses the procedural procedure for conducting pre-investigation checks on modern types of fraud, as well as the tactical features of its production. To solve the difficulties in the investigation of modern forms of fraud, such as masquerading as civil law torts, criteria for their delineation have been developed. It also provides a list of issues and circumstances to be established during the pre-investigation inspection, as well as the procedure for the seizure, inspection and registration of new types of evidence. Despite the computerization of all spheres of society, applying new types of fraud, the identification of new types of evidence and traces (electronic), the procedure for the seizure, inspection and registration of electronic evidence is not regulated procedurally (there is no concept of «electronic evidence»), as well as there is no unified approach to the production of certain investigative actions for detection and the withdrawal of such evidence. The article presents the opinions of scientists regarding the conceptual apparatus of «electronic evidence», as well as on the tactics of seizure, inspection and fixation of electronic evidence using modern technologies and software. In conclusion, proposals for amendments and additions to the criminal procedure legislation were put forward.*

Keywords: *fraud, fixation, electronic evidence, information and communication technologies, software, pre-investigation check.*

Введение

В мире огромное внимание уделяется повышению роли и защиты всех форм собственности, но посягательства на нее причиняют материальный ущерб физическим и юридическим лицам, так и государству. Так, доля корыстных преступлений, в частности мошенничества, в общей структуре преступности во всех странах мира является самой большой. Международная ассоциация сертифицированных экспертов по расследованию мошенничества ACFE (Association of Certified Fraud Examiners) обнародовала глобальный доклад по мошенничеству, который был составлен на основании изучения 2 504 случаев мошенничества, совершенных в 2020 году на территории 125 стран мира с общим ущербом в размере 3,6 млрд долларов. Самое большое количество мошенничества было установлено в США (46 %), затем в Африке (15 %), Азиатско-Тихоокеанском регионе (10 %), Западной Европе (7 %), Южной Азии, Латинской Америке, Восточной Европе и Западной/Центральной Азии по 5 % соответственно [1].

По статистике Генеральной прокуратуры Республики Узбекистан, в 2020 году наблюдался резкий рост мошенничества на 66 % [2], в особенности новых его видов. Согласно официальному заявлению Следственного департамента при МВД Республики Узбекистан, в 2020 году мошенничество, связанное с куплей-продажей земельных участков и домов, выросло на 13,9 %, а трудоустройство и зачисление на учебу – на 9 % [3].

Мошенничество является наиболее адаптирующимся и видоизменяющимся видом преступного посягательства, она быстро подстраивается под любую социальную и экономическую обстановку в обществе. Основной проблемой при его расследовании является трудность отграничения от гражданско-правового деликта.

Каждая новая форма мошенничества трактует своеобразную методику его расследования. К примеру, при расследовании дел касательно мошенничества с использованием информационно-коммуникационных сетей необходимо назначить судебную компьютерно-техническую экспертизу.

Качество расследования, установление истины и изобличение виновных лиц во многом зависят от методики расследования преступления. При этом, не владея достаточными теоретическими знаниями, невозможно установить истину и расследовать преступление в полной мере. В период стремительно развивающихся экономических отношений внедрение во все сферы жизни информационно-коммуникационных технологий способствует появлению все новых видов мошенничества, что требует постоянного совершенствования методики его расследования.

Президент Интерпола Ким Жонг Янг [4] отмечал, что использование технологий для совершения мошенничества не является новшеством, а Интернет и социальные сети, а также средства массовой информации сейчас дают возможность преступникам расширить географию их деятельности, диверсифицировать их цели и деятельность, часто даже без необходимости персонального взаимодействия и физического участия.

Целью исследования является разработка научно обоснованных рекомендаций по устранению существующих в судебно-следственной практике проблем, а также предложений для совершенствования уголовно-процессуального законодательства. Несмотря на наличие научных трудов касательно мошенничества, например среди зарубежных ученых, вопросы, связанные с раскрытием, расследованием и профилактикой традиционных, то есть не связанных с использованием современных средств и технологий, видов

мошенничеств изучали в своих научных работах Э. Вильямс [5, с. 13], А. Бозинис [6, с. 8], В. Альбрехт [7, с. 5] и многие другие.

Стоит отметить, что в Узбекистане Х.А. Тураббаев с своей работе на тему «Особенности расследования мошенничества» исследовал криминалистические элементы и традиционные особенности расследования мошенничества [8, с. 7]; Р.С. Алтиев в диссертации на тему «Уголовно-правовые и криминологические особенности мошенничества» комплексно изучил уголовно-правовые и криминологические особенности мошенничества [9, с. 4]. Из зарубежных ученых О.В. Волохова [10, с. 7] в своей диссертационной работе на тему «Особенности расследования мошенничества в отношении граждан» разработала методику расследования такого вида мошенничества, как «напёрстки», которое в данное время крайне редко встречается. Следует отметить, что данные научные труды не охватывают процессуальные и тактические аспекты производства доследственной проверки по видам мошенничества, что и предполагает актуальность статьи.

Материалы и методы

При осуществлении научного исследования были использованы общенаучные (логический, анализ, сравнение, синтез, обобщение, наблюдение), частнонаучные (статистический), специально-отраслевые (сравнительно-правовой, анализ уголовных дел, социологический опрос) методы исследования.

Результаты исследования

Для проведения всестороннего исследования были изучены материалы более 200 уголовных дел, более 100 судебных решений, статистические данные за 2015-2021 гг., проведен опрос среди 688 со-

трудников следственных органов МВД и судов.

В ходе проведенного исследования было установлено, что одной из сложностей в расследовании мошенничества является то, что оно маскируется под гражданско-правовые сделки, что и обуславливает проблемы в его выявлении, так как для этого необходим достаточный опыт и навыки для их отграничения. Согласно статистике, в 2020 году следственными подразделениями органов внутренних дел 10,4 % возбужденных уголовных дел было прекращено в связи с отсутствием признаков преступления с разъяснением сторонам о возможности обращения в суды по экономическим делам. Согласно проведенному опросу среди следователей и дознавателей, судей по уголовным делам¹, 63,8 % опрошенных участников указали о наличии проблем при отграничении мошенничества от невыполнения гражданско-правовых обязательств, и только 4,8 % указали на их отсутствие. В качестве причины возникновения данной путаницы и неправильного обращения граждан в правоохранительные органы по делам, в которых отсутствует состав мошенничества, 37,2 % указали на незнание лицами сущности долговых обязательств; 20,1 % – о доверчивости потерпевших; а 20,9 % – о правовой безграмотности потерпевших; 19,5 % показали, что проблемы возникают из-за отсутствия единого пособия по расследованию новых видов мошенничества, что и приводит к двоякому толкованию норм законодательства.

Для решения вопроса о возбуждении уголовного дела необходимо наличие повода и достаточных оснований, указывающих на признаки преступления, для уста-

¹ Опрос, проведенный среди следователей и дознавателей нижестоящих подразделений Следственного департамента при МВД Республики Узбекистан (среди следователей и дознавателей Республики Каракалпакстан, Кашкадарьинской, Бухарской, Сырдарьинской, Навоийской, Хорезмской, Андижанской, Ферганской, Наманганской, Джизакской областей), а также 57 судей по уголовным делам со всей республике в 2019 году.

новления которого проводится доследственная проверка. По справедливому замечанию Я.В. Комиссаровой, основным вопросом проводимой доследственной проверки является установление достаточных данных, указывающих на признаки преступления. Достаточность данных означает такую их совокупность и качество, которые позволяют сделать обоснованное предположение о совершении или подготовке к совершению преступления [11, с. 24].

Однако в уголовно-процессуальном законодательстве нет единого подхода и определения, какие данные являются достаточными для решения вопроса о возбуждении уголовного дела. Так как по каждому факту собираются документы, не свойственные для всех видов преступлений, наличие достаточных оснований должен решать сам дознаватель или следователь.

Мошенничество имеет высокий уровень латентности, так как многие потерпевшие не обращаются в правоохранительные органы либо обращаются слишком поздно, что затрудняет расследование, преступник может скрыться либо уничтожить следы преступления, потратить все денежные средства и ценности, что затруднит обеспечение возмещения материального ущерба.

По результатам опроса, в 58,8 % случаев обеспечение возмещения ущерба оказывается невозможным в связи с тем, что потерпевшие обращаются в правоохранительные органы слишком поздно¹. До подачи заявления, как правило, жертвы мошенничества просят мошенников вернуть им их имущество, ссылаясь на то, что они в случае возмещения ущерба откажутся от предъявленного иска. Так, согласно уголовному делу 2014 года Го-

сударственного архива Республики Каракалпакстан, потерпевшая в течение двух лет уговаривала мошенника вернуть ей взятые обманным путем денежные средства, в конце концов, устав от отговорок и не получив назад свои денежные средства, обратилась в правоохранительные органы. Остальные же потерпевшие были установлены инспектором профилактики, когда тот прибыл по месту жительства мошенника для истребования у него объяснительной по поступившему заявлению.

Даже в случае наличия повода для возбуждения уголовного дела, без достаточных оснований невозможно говорить о возбуждении уголовного дела. Но установить или уточнить, наличие каких именно оснований может считаться достаточным для каждого уголовного дела, невозможно. Как правильно утверждал Ю. Пилипенко, критериев «достаточности» данных для возбуждения уголовного дела в законодательстве нет, они субъективны для каждого следователя [12, с. 34].

Трудности возникают в связи с тем, что, несмотря на появление все новых видов мошенничеств, использование ими современных технологий, нет четко определенного круга обстоятельств, подлежащих установлению в ходе доследственной проверки, а также порядка изъятия, осмотра и фиксации электронных доказательств. Так, нельзя не согласиться с Е.А. Барсуковым и И.В. Белоусовым, которые в своих трудах говорили об отсутствии нормы, определявшей бы круг обстоятельств, которые подлежат установлению при поступлении заявления и определяют лишь условия для принятия решения о возбуждении или отказе в возбуждении уголовного дела [13, с. 39]. С другой стороны, ограничение следова-

¹ Опрос, проведенный среди следователей и дознавателей нижестоящих подразделений Следственного департамента при МВД Республики Узбекистан в 2019 году.

теля и дознавателя путем установления обязательных для установления обстоятельств представляется неверным в связи с тем, что, исходя из материалов проверки, он сам самостоятельно должен решать вопрос о возбуждении уголовного дела.

Немаловажной в ходе доследственной проверки является необходимость установления материальных и идеальных следов мошенничества, но не стоит забывать и об электронных следах. Электронные следы в основном оставляются мошенниками при использовании информационно-коммуникационных сетей, систем, технологий (переписки по сети Интернет, IP-адрес, сведения о вымышленном сайте, группах в социальных мессенджерах, таких как Telegram, Instagram, WhatsApp, о ложной рекламе, онлайн-благотворительность, онлайн-магазины).

Но, несмотря на то, что преступления с использованием информационных технологий встречаются все чаще, электронные доказательства, получаемые посредством современных технологий, а также порядок их осмотра, изъятия и оформления в уголовно-процессуальном законодательстве не урегулированы, также нет самого определения данного понятия, что приводит к разному толкованию и своевольному подходу при их изъятии.

Согласно действующему законодательству, доказательствами по делу являются любые сведения, имеющие значение по уголовному делу, основываясь на которые, уполномоченное законом лицо может вынести решение об обстоятельствах дела. Но, учитывая, что УПК Республики Узбекистан не предусматривает в качестве отдельного вида доказательства сведения в электронном виде (в форме компьютерной информации), то зачастую практики склонны относить ее к «иным видам доказательств», так как иначе ее трактовать не представляется возможным.

Б.А. Ражабов в своей работе отметил, что «прогресс науки и техники, стремительное развитие средств связи, осуществление отражения сведений в электронной цифровой форме, расширение возможностей использования этих сведений, а также необходимость создания возможностей использования в качестве доказательства сведений в данной форме также важны с точки зрения достижения эффективности» [14, с. 60].

Электронные доказательства или цифровые в соответствии с Национальным институтом юстиции США определяются как информация и данные, хранящиеся, полученные и переданные электронным устройством. Как отмечал А. Матчанов электронные доказательства – это фактические сведения, хранящиеся в материальном носителе, основу работы которого составляют информационные или иные инновационные технологии, представленные в электронном виде [15, с. 72].

Н.А. Зигура полагает, что компьютерная информация является новым видом доказательств, исходя из ее специфической формы, среды существования, механизма формирования и способа введения ее в качестве доказательств в уголовный процесс или способа преобразования ее в доказательство [16, с. 3]. Однако понятие «компьютерное доказательство» является крайне узким, так как не охватывает доказательства, которые были оставлены в электронном виде и составлены с помощью телефона, планшета или иных устройств. Более уместным будет обобщить данные доказательства в виде электронных. По мнению Д.Е. Лерна, цифровые доказательства – это информация и данные, представляющие ценность для расследования, которые хранятся, принимаются или передаются электронным устройством. Доказательством считаются данные или электронные устройства,

изъятые и защищенные для проверки [17, с. 3].

В ходе изучения судебно-следственной практики было установлено наличие проблем касательно изъятия, осмотра и фиксации электронных доказательств в ходе доследственной проверки. Аналогичная проблема существует также и в зарубежных государствах, таких как США. Зарубежные ученые Ш.Е. Гудисон, Р.С. Дэвис, Б.А. Джексон [18, с. 22] считают, что в США одной из проблем, встречающихся на практике, является трудность в управлении возможностью сбора и анализа цифровых доказательств с учетом темпов технологического прогресса, что требует разработки более стандартизированных сертификатов для экспертов-криминалистов, включая требования к непрерывному образованию. Они утверждали, что специалисты должны постоянно проходить курсы повышения квалификации в межведомственных и зарубежных семинарах-тренингах, мастер-классах, тренингах для изучения инновационных способов обнаружения и изъятия электронных доказательств. Так, они разработали пятиступенчатую систему способов изъятия электронных доказательств (табл.).

Каждый этап требует различного вида умений и оборудования для их изъятия. Следует учитывать, что изъятие электронных доказательств не является просто прокруткой текстовых данных или создание дубликатов жесткого диска путем его копирования.

Диапазон различных способов изъятия электронных доказательств из разных источников или типов устройств означает, что сбор значимой информации – многогранная задача, потенциально требующая умений создания, использования, управления возможностями технологического прогресса.

Таблица

Пятиступенчатая система методов изъятия электронных доказательств*

Метод изъятия доказательств вручную	Включает использование стандартных входов, входящих в комплект ли встроенных в устройство, например сенсорные экраны или клавиатуры. Это базовый метод, не требующий специальных знаний.
Логическое изъятие доказательств	Включает в себя внешнее компьютерное оборудование для передачи команд через код к назначенному устройству. Эксперты могут использовать различные инструменты подключения и программы обеспечения для подключения к устройству через свой компьютер, где извлекаемые данные должны отобразиться.
Чтение информации с карты памяти	Карта памяти – это место, где устройство хранит информацию об осуществленных действиях, для чтения и ввода информации. Этот уровень требует больших знаний и инструментов, чем предыдущие уровни, но потенциальные доказательства больше по количеству, и их труднее изменить подозреваемому.
“Chip off”, или изъятие чипа	Усовершенствованный метод изъятия и анализа электронного доказательства, которое включает в себя извлечение микросхем карт памяти из исследуемого устройства и последующее получение необработанных данных с помощью специального оборудования. Позволяет двоичному интеллекту создать полную картину практически любых устройств, даже если имеются серьезные повреждения.
Метод микрочтения	Наиболее усовершенствованный этап изъятия информации, который предполагает изъятие карты памяти с устройства и получение информации непосредственно с карты памяти без помощи устройства. Это аналогично микроскопическому исследованию компонентов или физическому извлечению жесткого диска, хотя к жесткому диску получить доступ легче.

* [18].

При совершении преступления с использованием электронного документа, электронной подписи или иного документа в электронном виде необходимо проведение некоторых следственных действий по его изъятию. К примеру, изъятие и осмотр электронного документа или электронного ключа на компьютере или съемном носителе информации (карта флэш-памяти), которое должно проходить с участием специалиста, а также с последующим протоколированием хода следственного действия.

Проблемы, встречающиеся на практике, существуют в связи с наличием в уголовно-процессуальном законодательстве пробелов. Без определения понятий электронного доказательства, электронных следов, электронной подписи невозможно установить, что именно следователь, дознаватель или специалист должны обнаружить, какие конкретно сведения могут иметь доказательственное значение и каков будет порядок изъятия данного вида доказательства, чтобы не допустить квалификации его в дальнейшем в виде недопустимых доказательств, то есть полученных с нарушением требований уголовно-процессуального законодательства. Данного мнения придерживались В.Б. Вехов, Б.П. Смагоринский, С.А. Ковалев [19, с. 10-19].

М.В. Горелов писал, что «При оценке электронных документов, представленных в качестве доказательств, должна учитываться ... правильность способа фиксации информации, ведь закрепление информации на современном источнике может отражаться на достоверности данного электронного доказательства» [20, с. 11]. Любые малейшие изменения могут привести доказательство в непригодность.

В случаях, когда мошенничество совершается с использованием глобальной сети Интернет (с входом в аккаунты, электронные ящики) либо с помощью со-

циальных мессенджеров, в этих случаях необходимо помнить, что осуществление входа возможно с любого устройства, который имеет выход в виртуальное пространство Интернет, будь то телефонный аппарат, компьютерная техника, планшет или иной гаджет), тогда даже в случае изъятия непосредственно телефона или другого устройства, злоумышленник может зайти с другого устройства и путем введения логина и пароля удалить все имеющиеся доказательства. Одно лишь изъятие устройств не говорит о сохранности и целостности электронных доказательств. Именно поэтому важно привлечение специалиста для поиска, обнаружения, изъятия, осмотра и надлежащего оформления электронных доказательств и записи на специальное запоминающее устройство для пресечения дистанционного доступа к нему, удаления либо внесения изменений. Ненадлежащим образом оформленное электронное доказательство может быть признано недопустимым, а злоумышленник может уйти от ответственности.

Другая проблема состоит в том, что, согласно статье 329 УПК Республики Узбекистан, в ходе доследственной проверки возможно проводить только *осмотр места происшествия*, но не предметов либо документов. Статья 198 УПК Республики Узбекистан предусматривает, что при представлении физическими либо юридическими лицами документов либо предметов дознаватель или следователь обязаны произвести осмотр представленных предметов для выяснения причастности к событию преступления и принять в случае, если он имеет доказательственное значение, в противном случае, немедленно после осмотра данные предметы или документы возвращаются по принадлежности.

Как отметил Б.А. Ражабов: «Несмотря на то, что согласно требованиям части

первой статьи 87 УПК определена возможность собирания доказательств путем производства следственных действий, однако закон запрещает производство всех определенных в УПК следственных действий во время доследственной проверки (ст. 329 УПК). Данное обстоятельство порождает определенные трудности при обеспечении соблюдения общих условий доказывания в судебно-следственной практике. В частности, при возникновении необходимости проведения ряда следственных действий перед возбуждением уголовного дела должностные лица, осуществляющие доказывание, вынуждены не соблюдать или обходить правила, связанные с общими условиями собирания доказательств» [14, с. 60].

Согласно требованиям УПК Республики Узбекистан, до возбуждения уголовного дела возможно производство осмотра места происшествия. Но цифровая информация, хранимая на электронных носителях информации, не относится ни к одному из вышеперечисленных. Отнесение электронной информации к предмету и документам невозможно ввиду нематериальности и отсутствия признака осязаемости.

Кроме того, распространенной ошибкой на практике является признание скриншотов и распечаток переписки вещественными доказательствами. Признание электронных следов вещественными представляется не совсем верным, так как данный вид следов нельзя отнести ни к материальным (не имеет отпечатков на материальном носителе), ни к идеальным (не находится в памяти либо сознании человека). Данный вид следов имеет специфические критерии, к примеру, находясь в памяти ЭВМ либо иного устройства, доступного для восприятия и считывания посредством ЭВМ, с использованием принтера может быть распечатана на бумажный носитель, то есть на материаль-

ный объект, но без доступа к электричеству получение доступа к данным следам невозможно.

По современным и традиционным видам мошенничества в случаях, когда основным источником доказательств служит расписка либо переписка в социальных мессенджерах, а производство осмотра места происшествия не имеет смысла в связи с поздним обращением потерпевшего в правоохранительные органы, то производство осмотра предмета либо документа может нести важное доказательственное значение, и запрет на его осуществление может привести к фальсификации документов, незаконному отказу в возбуждении уголовного дела, обходу данного «правила» и, как следствие, нарушению требований законодательства.

Данная проблема может возникнуть и в случае, когда потерпевший обращается в правоохранительные органы в связи с передачей по социальным мессенджерам денежных средств мошеннику. М.С. Садырова также упоминала о необходимости введения отдельного следственного действия в виде осмотра электронного устройства [21, с. 279].

Кроме того, законодателем определен круг следственных действий, проведение которых возможно до возбуждения уголовного дела. В остальном лицо, осуществляющее доследственную проверку, следователь или дознаватель, имеет свободу в использовании того или иного метода, тактики при собирании доказательств. Многие не уделяют должного внимания важности такого этапа судопроизводства, как «доследственная проверка», а ведь основная масса вещественных, письменных и электронных доказательств собирается именно на данном этапе.

Использование современных технологий при его производстве также считается важным критерием эффективности проводимых действий. К примеру, в

качестве современного способа проведения опроса может быть проведение и фиксация его хода в специальных комнатах, которыми в данный период времени оборудуются здания территориальных подразделений органов внутренних дел. Необходимо использовать все силы и средства для установления истины, в каждом случае по заявлениям о мошенничестве необходимо направить запросы в территориальные отделы по земельным ресурсам и государственному кадастру районов или городов для установления наличия имущества подозреваемого лица для решения вопроса обеспечения материального ущерба.

Как отметила А.Р. Арсланова, «одним из основных моментов для формирования сведений, содержащих признаки состава преступления, в ходе доследственной проверки является процессуальное средство проверки, в виде изъятия и приобщения к материалам проверки предметов и документов, которые после возбуждения уголовного дела могут приобретать статус вещественных доказательств по уголовному делу, то есть нести в себе важнейшие сведения для доказывания по уголовному делу» [22, с. 247].

Важность данного этапа судопроизводства отстаивал в своих трудах и С.А. Новиков, утверждая, что материалы доследственной проверки имеют самостоятельное доказательственное значение и в соответствии с принципом свободной оценки доказательств могут играть важную роль для точного установления значимых обстоятельств совершенного преступления [23, с. 74]. Именно поэтому правильное получение и оформление документов, полученных в ходе доследственной проверки, гарантирует возможность их использования в качестве доказательств.

В случаях, связанных с мошенничеством с использованием информационно-коммуникационных сетей и систем, не-

обходимо установление сотрудничества и привлечение высококвалифицированных специалистов из компаний, чья непосредственная работа связана с обнаружением новых вирусных программ и разработкой антивирусов для борьбы с вредоносными программами, к примеру «Лаборатория Касперского». UzCard на своем официальном сайте объявила об обнаружении их специалистами каналов в Telegram, созданных кибермошенниками по привлечению граждан в незаконный бизнес за счет перевода денежных средств через мобильные приложения (Payme, Click, Paynet), заверив, что всячески будут оказывать содействие правоохранительным органам в установлении мошенников [24].

По изученным материалам доследственной проверки и уголовным делам касательно новых видов мошенничества (фишинг, кибермошенничество), по которым отсутствует методика расследования, в большинстве случаев сбор материалов доследственной проверки ограничивался лишь приобщением заявления и объяснительной записки потерпевшего, истребованием документов (детализаций звонков, скриншотов переписок в социальных сетях, квитанций о перечислении денежных средств, копии транзакций и т. д.). С данными материалами рассматривался вопрос об отказе в возбуждении уголовного дела, нежели в возбуждении и полноценном расследовании него, посредством производства более широкого спектра следственных действий, которые возможно провести во время предварительного следствия. Стоит отметить, что, согласно справке Следственного департамента при МВД Республики Узбекистан от 21.01.2021 года № 18-490, количество отказов в возбуждении уголовного дела на основании статьи 83 УПК Республики Узбекистан по заявлениям о мошенничестве в 2020 году по республике увеличилось на 54 %.

Анализ результатов исследования

Существуют некоторые проблемы в ходе доследственной проверки по заявлениям о современных видах мошенничества. Во-первых, мошенничеству, совершенному с использованием информационно-коммуникационных технологий, сетей и систем характерно отсутствие идеальных следов мошенничества. Так, если мошенничество совершено в социальных сетях, то минимизируется визуальный контакт (по Telegram, к примеру, невозможно даже увидеть номер телефона аккаунта либо его профиль в целом, а в дальнейшем вовсе удалить всю переписку в одностороннем порядке). Также есть возможность получить конфиденциальную информацию (код подтверждения, логин и пароль, данные платежной карты), находясь в значительном отдалении от жертвы преступления (в некоторых случаях даже находясь на территории другой страны), что делает фактически трудно достижимым установление их личности.

Во-вторых, трудности в установлении личности мошенника, так как современные возможности для онлайн-передачи денежных средств посредством систем онлайн-банкинга (Click, Payme, Paynet) либо электронных платежных систем (UzCard, Humo), электронных денег (WebMoney, QiWi, ЮMoney) позволяют получить доступ к ним, и без ведома владельца платежных карт снять деньги со счета через банкоматы либо перенаправить на другие счета, в основном на офшорные банковские счета (уголовное дело № 1-2012-2001/78 архива суда по уголовным делам Румитанского района Бухарской области 2021 года).

В-третьих, мошенники, особенно фишеры, используют невнимательность и неосмотрительность потерпевших лиц в виртуальном пространстве, и отсутствие информационной грамотности касатель-

но возможностей современных IT-технологий. Однако мошенники также используют тактические приемы для снижения концентрации внимания жертв, чтобы те перешли по поддельной ссылке либо ввели логин и пароль на стороннем сайте («Спешите, вы выиграли в акции!», «Срок действия один день!», «Осталось 2 часа!», «Количество ограничено!» и т.д.).

В-четвертых, по результатам доследственной проверки должностные лица принимали решение об отказе в возбуждении уголовного дела, даже при наличии признаков преступления, ссылаясь на то, что раскрыть преступление не удастся в связи с совершением преступления лицом, находящимся на территории иностранного государства, переводом денежных средств на офшорные счета государств, с которыми не был подписан меморандум о сотрудничестве правоохранительных органов. Так, по материалам доследственной проверки архива Следственного управления МВД при Республике Каракалпакстан 2017 года, зарегистрированным в Форме № 1 № 2000 ОВД города Нукуса, было установлено, что через группу в социальном мессенджере WhatsApp потерпевшая заказала 2 телефона марки iPhone по цене одного (акция «Только сегодня! 2 телефона по цене 1-го!») и сделала денежный перевод на имя М. (копия паспорта и копия квитанции о переводе денежных средств была прикреплена) в город Москву через платежную систему Юнистрим. После получения денежных средств группа была удалена, а на связь с мошенником выйти не удалось. По данному факту было принято решение об отказе в возбуждении уголовного дела, которое затем было отменено прокурором.

В-пятых, по некоторым фактам мошенничества не направлялись запросы в банки или организации систем онлайн-банкинга (Click, Payme, Paynet) либо элек-

тронных систем платежа (UzCard, Humo), осуществляющие денежные переводы, ссылаясь на необходимость получения санкции прокурора для получения информации, составляющей банковскую тайну, либо требования времени для направления постановления в Центральный банк Узбекистана либо Главные офисы иных банков в связи с совершением мошенничества злоумышленником, находясь в другой части страны или денежного перевода на офшорные счета стран и отсутствия заключенных межгосударственных меморандумов с ними.

В-шестых, материалы следственной проверки либо заявления физических лиц неоднократно перенаправлялись из одной области/района в другие якобы по территориальной подследственности, ссылаясь на местожителство мошенника либо заявителя, место обналичивания или перевода денежных средств. Так, если мошенничество совершено в одной области, а мошенник находится в другой области, решается вопрос о территориальный подследственности.

Выводы

Проведенное исследование и сравнительно-правой анализ норм УПК и существующей судебно-следственной практики позволили сформировать круг обстоятельств, подлежащих выяснению в ходе следственной проверки по факту совершения мошенничества:

- завладение имуществом или приобретение права на имущество было совершено противоправно с ложным обещанием или введением в заблуждение;
- чуждость и отсутствие прав на распоряжение имуществом, которым завладел мошенник;
- имущество отчуждено в пользу мошенника либо третьих лиц;
- преступный умысел – корысть, то есть желание обогатиться или получить какую-либо материальную выгоду;

- завладение имуществом преследовало цель невозвращение материальных ценностей или неадекватное возвращение.

Учитывая, что электронные доказательства являются новым видом доказательств, отсюда вытекает необходимость его законодательного урегулирования для устранения возникающих коллизий в законодательстве, устранения ошибок при квалификации и производстве следственных действий в ходе следственной проверки, в связи с чем предлагается внести изменения в УПК Республики Узбекистан:

- часть 1 статьи 26 УПК Республики Узбекистан после слов «вещественные» дополнить словами «электронные»;
- часть 2 статьи 81 УПК Республики Узбекистан после слов «вещественными» дополнить словами «электронными»;
- часть 3 статьи 90 УПК Республики Узбекистан после слов «материальных» дополнить словами «или электронных»;
- главу 25 УПК Республики Узбекистан переименовать и изложить в следующей редакции: *«Приобщение к делу предметов и документов в качестве вещественных, электронных и письменных доказательств»;*
- дополнить УПК Республики Узбекистан статьей 204¹ и изложить ее в следующей редакции:

«Статья 204¹. Электронные доказательства

Электронными доказательствами являются сведения, данные или информация, хранящиеся или передаваемые в цифровой форме, имеющие прямое или косвенное отношение к событию преступления, отражающие обстоятельства совершенного преступления, изъятые и оформленные в соответствии с нормами УПК»;

- изложить статью 205 УПК Республики Узбекистан в следующей редакции:

«Статья 205. Способы получения вещественных, электронных и письменных доказательств»

Предметы, документы, электронные и иные записи, используемые как вещественные, электронные или письменные доказательства, могут быть получены при осмотре места происшествия или иной местности, помещения, компьютерных техник, аппаратных устройств, информационно-коммуникационных технологий, систем, сетей или программ обеспечения при предъявлении для опознания, освидетельствовании, эксгумации трупа, изъятии образцов для экспертного исследования, проверке показания на месте, производстве выемки, обыска или эксперимента либо они могут быть представлены дознавателю, следователю или суду в порядке, предусмотренном статьями 198–202 настоящего Кодекса»;

- изложить статью 208¹ УПК Республики Узбекистан в следующей редакции:

«Статья 208¹. Хранение и пересылка электронных доказательств»

При осмотре и изъятии электронных носителей информации обязательно участие специалиста для записи их на специальные записывающие устройства с использованием необходимых программ для обеспечения целостности и предупреждения внесения последующих изменений, их утраты или повреждения. Ход и результаты осмотра электронных носителей информации должны фиксироваться в протоколе. Электронные доказательства, изъятые и хранящиеся в установленном порядке, прилагаются к материалам дела»;

- часть 1 статьи 135 УПК Республики Узбекистан после слов «предметов» дополнить словами «информации, хранящейся или передаваемой в цифровой форме»;

- часть 3 статьи 135 УПК Республики Узбекистан после слов «предметы» до-

полнить словами «информация, хранящаяся или передаваемая в цифровой форме».

- дополнить УПК Республики Узбекистан статьей 140¹ и изложить ее в следующей редакции:

«Статья 140¹. Осмотр информации, хранящейся или передаваемой в цифровой форме»

Должностное лицо органа, осуществляющего доследственную проверку, дознаватель, следователь и суд осматривают информацию, хранящуюся или передаваемую в цифровой форме по месту их обнаружения с обязательным участием специалиста, а в дальнейшем, если для осмотра требуются продолжительное время или дополнительные технические средства, – по месту производства дознания, предварительного следствия или судебного разбирательства.

Осмотр обязательно должен производиться с участием специалиста и применением технических средств с соблюдением правил по предотвращению утраты, повреждения или внесения изменений в информацию, хранящуюся или передаваемую в цифровой форме.

В случаях, не терпящих отлагательства, осмотр информации, хранящейся или передаваемой в цифровой форме, допускается до возбуждения уголовного дела».

Необходимо сформулировать авторское определение понятия электронного доказательства: электронное доказательство – это сведения, данные или информация, хранящиеся или передаваемые в цифровой форме, имеющие прямое или косвенное отношение к событию преступления, отражающие обстоятельства совершенного преступления, изъятые и оформленные в соответствии с нормами УПК.

На наш взгляд, также необходимо сформулировать авторское определение понятия электронных следов: электронные следы – это следы, которые отражают процесс совершения определенных

действий в виртуальном пространстве, а также на носителях электронной информации в форме доступной для чтения ЭВМ.

Разработанные в ходе научного исследования предложения послужат устранению имеющихся в судебно-следственной

практике ошибок, усовершенствованию действующего уголовно-процессуального законодательства, а также обеспечению качественного производства доследственной проверки уполномоченными лицами.

REFERENCES

1. The 2020 Report to the Nations – the ACFE's 11th study on the costs and effects of occupational fraud. 2020 Global study on occupational fraud and abuse. P. 4.
2. Spravka General'noy prokuratury Respubliki Uzbekistan ot 10.02.2020 [Certificate of the General Prosecutor's Office of the Republic of Uzbekistan dated 2020, February 10].
3. Spravka Sledstvennogo departamenta pri MVD Respubliki Uzbekistan. Svedeniya o sovershennykh moshennichestvakh za 2020 god [Certificate of the Investigation Department under the Ministry of Internal Affairs of the Republic of Uzbekistan. Information about committed scams for 2020.]. Available at: <https://tergov.uz/ru/news/svedeniya-o-sovershennykh-moshennichestvah-za-2020-god/> (accessed 12.02.2021).
4. Experts gather to tackle telecom fraud and other scams. Available at: <https://www.interpol.int/News-and-Events/News/2019/Experts-gather-to-tackle-telecom-fraud-and-other-scams/>.
5. Williams J., Joinson A.N. Developing a measure of information seeking about phishing. *Journal of Cybersecurity*, 2020, vol. 6, no. 1, p. 13.
6. Bozinis A. Countering Fraud and Corruption. Portsmouth University, 2014, p. 8.
7. Albrecht W.S., Albrecht C.C., Albrecht C.D. Fraud Examination. 3rd ed., Thomson, South-Western, 2009, p. 8. Available at: <https://books.google.co.id/books?id=R6q5BwAAQBAJ&printsec=copyright&hl=id#v=onepage&q&f=false/>.
8. Turabbayev H.A. Features of fraud investigation. Abstract of PhD thesis. Tashkent, 2001, p. 7.
9. Altiev R.S. Criminal-legal and criminological aspects of fraud. Abstract of PhD thesis. Tashkent, 2020, p. 4.
10. Volokhova O.V. Features of the investigation of fraud committed against citizens. Abstract of PhD thesis. Moscow, 2003, p. 7. Available at: <https://www.dissercat.com/content/osobennosti-rassledovaniya-moshennichestva-sovershennogo-v-otnoshenii-grazhdan/>.
11. Komissarova Ya.V. Criminalistic study of personality. A scientific and practical guide for masters. Moscow, Prospect Publ., 2017, 24 p. Available at: <http://lib.lawinstitut.ru/ru-virtualexposition/newbooks/82-932176.pdf/>.
12. Pilipenko Yu. Sanctions for "criminal pressure" on business: will the security forces remain unpunished? *Practical accounting*, 2017, no. 1, p. 34. Available at: <http://base.garant.ru/>.
13. Barsukov E.A., Belousov I.V. The subject of proof at the stage of initiation of a criminal case. *Central Scientific Bulletin*, 2017, no. 11, pp. 39-41. Available at: <http://cscb.su/n / 021101/021101022.html/>.
14. Razhabov B.A. Problems associated with ensuring compliance with the general conditions of proof in the criminal process of the Republic of Uzbekistan. *Problems of modern science and education*, 2020, no. 4 (149), p. 60. Available at: <https://cyberleninka.ru/article/n/problemny-svyazannye-s-obespecheniem-soblyudeniya-obshchih-usloviy-dokazyvaniya-v-ugolovnom-protseste-respubliki-uzbekistan/>.
15. Matchanov A.A. About the peculiarities of obtaining evidence in electronic (digital) form in the investigation of cybercrime. Mutual legal assistance in obtaining electronic evidence and cross-border

investigations of crimes. A handbook based on the results of a regional seminar for criminal justice practitioners in Central Asia. Tashkent, 2020, p. 72.

16. Zigura N.A. Computer information as a type of evidence in the criminal process of Russia. Abstract of PhD thesis. Chelyabinsk, 2010. Available at: <https://www.dissercat.com/content/kompyuternaya-informatsiya-kak-vid-dokazatelstv-v-ugolovnom-protsesse-rossii/>.

17. Learner D.E. Electronic crime scene investigation. New York, Nova Science Publ. Inc., 2009, p. 3.

18. Goodison S.E., Davis R.C., Jackson B.A. Digital evidence and the U.S. criminal justice system identifying technology and other needs to more effectively acquire and utilize digital evidence. P. 22. Available at: http://www.rand.org/pubs/research_reports/RR890.html/.

19. Vekhov V.B., Smagorinsky B.P., Kovalev S.A. Electronic traces in the system of criminalistics. *Forensic examination*, 2016, no. 2 (46), pp. 10-19.

20. Gorelov M.V. Electronic evidence in civil proceedings of Russia: questions of theory and practice. Abstract of PhD thesis. Yekaterinburg, 2005, p. 11. Available at: <https://www.dissercat.com/content/elektronnye-dokazatelstva-v-grazhdanskom-sudoproizvodstve-rossii-voprosy-teorii-i-praktiki/>.

21. Sadyrova M.S., Menzhega M.M. Inspection of electronic devices as an independent investigative action. Legal sciences: problems and prospects. Proceedings of the IV International Scientific Conference. Kazan, 2016, May. Kazan, Buk, 2016, pp. 279-281. Available at: <https://moluch.ru/conf/law/archive/181/10391/> (accessed 15.02.2021).

22. Arslanova A.R. Problems of seizure of objects and documents before the initiation of a criminal case. *Gaps in Russian legislation*, 2015, p. 247. Available at: <https://cyberleninka.ru/article/n/problem-izyatiya-predmetov-i-dokumentov-do-vozbuzhdeniya-ugolovnogo-dela/> (accessed 17.10.2019).

23. Novikov S.A. Materials of pre-investigation verification in proving criminal cases: current problems and new approaches. *Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia*, 2013, no. 3 (59), p. 74. Available at: <https://cyberleninka.ru/article/n/materialy-dosledstvennoy-proverki-v-dokazyvanii-po-ugolovnym-delam-aktualnye-problemy-i-novye-podhody/>.

24. Osteregajtes moshennikov [Beware of scammers]. Available at: <https://uzcard.uz/index.php/ru/novosti-uzcard/item/878-osteregajtes-moshennikov/>.

YURISPRUDENSIYA

HUQUQIY ILMIY-AMALIY JURNALI

3 / 2022

BOSH MUHARRIR:

Xodjayev Baxshillo Kamolovich

Ilmiy ishlar va innovatsiyalar bo'yicha prorektor,
y.f.d., dotsent

BOSH MUHARRIR O'RINBOSARI:

Ikrom Ergashev

Ilmiy boshqarma boshlig'i, yuridik fanlar bo'yicha
falsafa doktori, dotsent – bosh muharrir o'rinbosari

Mas'ul muharrir: D. Xudoynazarov

Muharrirlar: Sh. Jahonov, K. Abduvaliyeva,
Y. Yarmolik, F. Muhammadiyeva, Sh. Yusupova

Texnik muharrirlar: U. Sapayev, D. Rajapov

Tahririyat manzili:

100047. Toshkent shahar, Sayilgoh ko'chasi, 35.

Tel.: (0371) 233-66-36, 233-41-09.

Faks: (0371) 233-37-48.

Web-sayt: www.tsul.uz

E-mail: lawjournal@tsul.uz

E-mail: tn.tdyu@mail.ru

Obuna indeksi: 1387.

Jurnal 19.07.2022-yilda tipografiyaga topshirildi.

Qog'oz bichimi: A4. Shartli 23,28 b.t. Adadi: 100.

Buyurtma raqami: 47.

TDYU tipografiyasida chop etildi.