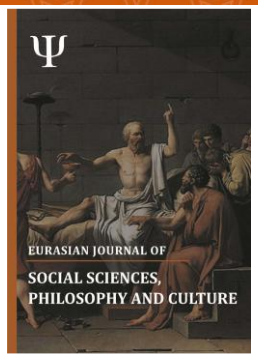
EURASIAN JOURNAL OF SOCIAL SCIENCES, PHILOSOPHY AND CULTURE
Innovative Academy Research Support Center
IF = 9.3 www.in-academy.uz/index.php/ejsspc



FACTUAL CONTROL OVER DIGITAL INSTRUMENTS AS AN EVIDENTIARY CRITERION IN CYBERCRIME INVESTIGATIONS

AYBEK ORAZBAYEVICH KHALMURATOV
Independent Researcher, Law Enforcement Academy of the Republic of Uzbekistan
bekbayevich@proacademy.uz
https://doi.org/10.5281/zenodo.21065611

ARTICLE INFO
Received: 02nd June 2026
Accepted: 08th June 2026
Online: 09th June 2026
KEYWORDS
Cybercrime; digital evidence; factual control; digital trace; crypto-assets.

ABSTRACT
This article examines factual control over a digital instrument as a key evidentiary issue in cybercrime investigations. It argues that formal ownership of a bank card, SIM card, account, IP address, electronic wallet, or crypto wallet cannot by itself establish a person's involvement, unless supported by technical, registration, behavioural, and financial-transactional indicators. The article proposes a verification model based on the sequence "instrument – access – action – disposition – benefit" to link digital traces with the actual user of the relevant digital instrument.

ФАКТИЧЕСКИЙ КОНТРОЛЬ НАД ЦИФРОВЫМИ ИНСТРУМЕНТАМИ КАК ДОКАЗАТЕЛЬСТВЕННЫЙ КРИТЕРИЙ

ХАЛМУРАТОВ АЙБЕК ОРАЗБАЕВИЧ
Самостоятельный соискатель Правоохранительной академии Республики Узбекистан
bekbayevich@proacademy.uz
https://doi.org/10.5281/zenodo.21065611

ARTICLE INFO
Received: 02nd June 2026
Accepted: 08th June 2026
Online: 09th June 2026
KEYWORDS
Киберпреступление; цифровое доказательство; фактический контроль; цифровой след; криптоактивы.

ABSTRACT
В статье рассматривается фактический контроль над цифровым инструментом как ключевая доказательственная проблема при расследовании киберпреступлений. Обосновывается, что формальная принадлежность банковской карты, SIM-карты, аккаунта, IP-адреса, электронного кошелька или криптокошелька сама по себе не может устанавливать причастность лица без подтверждения техническими, регистрационными, поведенческими и финансово-транзакционными признаками. Предлагается проверочная модель "инструмент – доступ – действие – распоряжение – выгода", позволяющая связать цифровые следы с фактическим пользователем соответствующего цифрового инструмента.

EURASIAN JOURNAL OF SOCIAL SCIENCES, PHILOSOPHY AND CULTURE
Innovative Academy Research Support Center
IF = 9.3 www.in-academy.uz/index.php/ejsspc

RAQAMLI VOSITALAR USTIDAN FAKTIK NAZORAT KIBERJINOYATLARNI TERGOV QILISHDA ISBOTLOVCHI MEZON SIFATIDA

XALMURATOV AYBEK ORAZBAYEVICH
O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi mustaqil tadqiqotchisi
bekbayevich@proacademy.uz
https://doi.org/10.5281/zenodo.21065611

ARTICLE INFO

Received: 02nd June 2026
Accepted: 08th June 2026
Online: 09th June 2026

KEYWORDS

Kiberjinoyat; raqamli dalil; faktik nazorat; raqamli iz; kriptoaktivlar.

ABSTRACT

Maqolada raqamli vosita ustidan faktik nazorat kiberjinoyatlarni tergov qilishdagi muhim isbotlash muammosi sifatida tahlil qilinadi. Bank kartasi, SIM-karta, akkaunt, IP-manzil, elektron hamyon yoki kriptohamyonning rasmiy tegishliligi shaxsning jinoyatga aloqadorligini o‘z-o‘zidan tasdiqlay olmasligi, bunday xulosa texnik, ro‘yxatga olishga oid, xulq-atvor va moliyaviy-tranzaksion belgilar bilan tasdiqlanishi zarurligi asoslantiriladi. Maqolada raqamli izlarni tegishli raqamli vositaning faktik foydalanuvchisi bilan bog‘lashga xizmat qiluvchi “vosita – kirish – harakat – tasarruf etish – manfaat” tekshiruv modeli taklif etiladi.

Современное расследование киберпреступлений сталкивается не только с необходимостью обнаружения цифровых следов, но и с проблемой их правильной уголовно-процессуальной и криминалистической интерпретации. Банковская карта, SIM-карта, аккаунт в мессенджере, IP-адрес, электронный кошелёк, криптокошелёк или криптоадрес позволяют установить определённый цифровой либо финансовый инструмент, использованный в преступной схеме. Однако сам по себе такой инструмент не раскрывает, кто фактически им управлял, кто распоряжался полученными данными или средствами, и кто имел реальную возможность совершить юридически значимое цифровое действие.

Актуальность данной проблемы усиливается развитием правового режима цифровых доказательств в Республике Узбекистан. Законом Республики Узбекистан от 21 ноября 2024 года № ЗРУ-1003 уголовно-процессуальное законодательство дополнено положениями об электронных данных и цифровых доказательствах. В УПК Республики Узбекистан электронными данными признаются данные, создаваемые, обрабатываемые и хранимые с использованием электронных устройств, информационных систем и информационных технологий, а цифровыми доказательствами – электронные данные, содержащие сведения об обстоятельствах, имеющих значение для дела [1]. Эти изменения создали нормативную основу для работы с цифровой

информацией, но не устранили криминалистический вопрос о связи цифрового объекта с конкретным лицом.

Практическая значимость указанного вопроса подтверждается динамикой преступлений, совершаемых с использованием информационных технологий. По данным аналитических материалов Правоохранительной академии Республики Узбекистан, количество таких преступлений в 2023 году составило 5 399, в 2024 году – 58 698, а за восемь месяцев 2025 года – 38 195 [2]. Эти сведения указывают не только на количественный рост соответствующей категории преступлений, но и на усложнение задач доследственной проверки, предварительного следствия, экспертного исследования и оценки цифровой информации.

Центральная проблема состоит в том, что формальная принадлежность цифрового или финансового инструмента не всегда совпадает с фактическим контролем над ним. Банковская карта может быть оформлена на одно лицо, но использоваться другим участником схемы; SIM-карта может быть передана третьему лицу либо применяться для получения одноразовых кодов; аккаунт может быть создан, продан, взломан или администрироваться удалённо; IP-адрес может отражать подключение через публичную сеть, VPN-сервис или иное техническое средство; криптокошелёк может контролироваться не формальным владельцем, а лицом, обладающим seed-фразой, приватным ключом, логином или паролем. При таких условиях отождествление владельца карты, номера, аккаунта, IP-адреса или криптокошелька с фактическим исполнителем создаёт риск преждевременной персонализации следственной версии.

Цель статьи заключается в обосновании необходимости рассматривать установление фактического контроля над цифровым инструментом как самостоятельный элемент доказывания при расследовании киберпреступлений. Для достижения этой цели решаются следующие задачи: анализируются научные подходы к понятию киберпреступления как криминалистической категории; уточняется содержание понятий “цифровой инструмент”, “цифровой след” и “фактический контроль”; показывается практическое проявление проблемы при использовании банковских карт, SIM-карт, аккаунтов и криптоактивов; предлагается методическая модель проверки фактического контроля.

Методологическую основу статьи составляют формально-юридический, системно-структурный, сравнительно-аналитический и криминалистический методы, а также метод научного моделирования.

Для обоснования категории фактического контроля необходимо исходить из того, что понятие “киберпреступление” в уголовном процессе и криминалистике не совпадает с его бытовым или сугубо

техническим употреблением. В уголовно-правовом смысле внимание сосредоточено на составе преступления, объекте посягательства, форме вины, последствиях и квалифицирующих признаках. Для расследования этого недостаточно, поскольку следователь устанавливает не только юридическую модель деяния, но и механизм его отражения в цифровой среде: где образовались следы, у кого они находятся, каким способом могут быть получены, сохранены, проверены и процессуально закреплены.

В научной литературе можно выделить несколько подходов к определению киберпреступления. Первый подход является узким: к киберпреступлениям относят преимущественно деяния, непосредственно посягающие на компьютерную информацию, информационные системы либо безопасность их функционирования. Его преимущество состоит в юридической определённости, однако он не охватывает значительный массив преступлений, где цифровая среда используется как способ совершения, сокрытия или последующего распоряжения преступным результатом. Второй подход является расширительным: он включает любые преступления, совершённые с использованием информационных технологий. Такая позиция отражает современную трансформацию преступности, но при чрезмерно широком применении размывает границу между собственно киберпреступлением и общеуголовным деянием, при совершении которого цифровое средство использовалось вспомогательно. Третий подход имеет криминалистический характер: киберпреступление рассматривается через влияние цифровой среды на способ подготовки, совершения, сокрытия деяния, образование следов, распределение доказательственной информации и тактику её получения [3].

Для целей настоящей статьи предпочтительным является третий подход. Киберпреступление следует рассматривать как криминалистическую категорию не потому, что она заменяет уголовно-правовую квалификацию, а потому, что она позволяет определить доказательственную модель расследования. В этом смысле значение имеет не сам факт использования телефона, компьютера, банковского приложения или сети Интернет, а то, изменяет ли цифровая среда механизм преступления и порядок доказывания. Если цифровой элемент не влияет на способ совершения, следовую картину и источники информации, он не образует самостоятельной криминалистической специфики. Если же без цифровых данных невозможно установить событие, способ, участника, маршрут средств или связь между действиями лиц, преступление приобретает значение объекта специальной методики расследования [4].

В рамках указанного подхода требуется определить понятие

цифрового инструмента. Под цифровым инструментом в настоящей статье понимается техническое, программное, коммуникационное, платёжное или криптоактивное средство, с помощью которого лицо получает доступ к цифровой среде, совершает юридически значимое действие, управляет информацией, распоряжается денежными средствами либо скрывает связь между собой и преступным результатом. К таким инструментам относятся мобильное устройство, компьютер, SIM-карта, банковская карта, мобильное приложение, аккаунт, электронный кошелёк, криптокошелёк, доменное имя, IP-соединение, облачный сервис, платёжный профиль, средство аутентификации, пароль, одноразовый код, приватный ключ и seed-фраза. Перечень не является закрытым, поскольку криминалистическое значение имеет не форма объекта, а его роль в механизме преступления.

Цифровой инструмент необходимо отличать от цифрового следа. Инструмент используется для действия; след отражает это действие в электронной среде. Вход в аккаунт, изменение пароля, получение SMS-кода, переход по фишинговой ссылке, платёжная операция, подключение к сети, создание файла, удаление переписки, транзакция с криптоактивом или передача данных доступа образуют цифровые следы. Однако цифровой след имеет первоначально ориентирующее значение. Он показывает, что определённое действие, событие или состояние было зафиксировано в цифровой среде, но сам по себе не устанавливает, кто именно совершил это действие, обладал ли он доступом к инструменту, действовал лично, через посредника, удалённо или с использованием чужих реквизитов.

Доказательственное значение цифрового следа возникает после установления его источника, проверки целостности, законного получения, процессуального закрепления, относимости к расследуемому событию и связи с конкретным субъектом. Электронные данные, лог входа, IP-адрес, банковская транзакция, сведения об аккаунте или хеш криптооперации могут подтвердить наличие цифрового события, но не всегда подтверждают личность фактического пользователя. Между цифровым следом и выводом о причастности лица должен находиться проверочный этап, включающий сопоставление технических, регистрационных, поведенческих, телекоммуникационных и финансовых данных.

На этой основе формулируется понятие фактического контроля. Под фактическим контролем над цифровым инструментом следует понимать подтверждённую совокупностью доказательственных данных реальную возможность лица использовать соответствующий инструмент для доступа, управления, подтверждения операции, передачи информации, распоряжения денежными средствами или

криптоактивом независимо от того, является ли это лицо формальным владельцем, зарегистрированным пользователем либо держателем соответствующего реквизита. Фактический контроль может выражаться в физическом владении устройством, знании пароля, использовании PIN-кода, получении одноразового SMS-кода, подтверждении операции через push-уведомление, доступе к аккаунту, управлении банковским приложением, распоряжении картой, использовании SIM-карты, владении приватным ключом, seed-фразой или иным средством доступа.

Такое понимание позволяет отделить формальную принадлежность цифрового инструмента от реального управления им. Банковская карта может быть зарегистрирована на одно лицо, но использоваться другим лицом через мобильное приложение или переданные реквизиты. SIM-карта может быть оформлена на формального абонента, но применяться третьим лицом для регистрации аккаунта, получения SMS-кодов или подтверждения платежей. Аккаунт может быть создан на один номер, но фактически управляться иным пользователем. IP-адрес может указывать на сетевое соединение, но не всегда индивидуализирует лицо, поскольку подключение может осуществляться через публичную сеть, VPN-сервис, прокси, общее устройство или удалённый доступ. Криптокошелёк может быть связан с определённым адресом, но распоряжение активом осуществляет тот, кто обладает приватным ключом, seed-фразой, логином или паролем.

Следовательно, формальная регистрация карты, номера телефона, аккаунта, электронного кошелька или криптокошелька не может рассматриваться как самостоятельное подтверждение причастности лица. Она является исходным ориентиром расследования, но не завершённым доказательственным выводом. В противном случае возникает риск подмены фактического пользователя формальным владельцем, что создаёт повышенный риск неправильной оценки роли лица по делам, где используются подставные лица, “дроп”-инструменты, переданные аккаунты, дистанционное управление, анонимизирующие сервисы и криптоактивные средства. Для обоснованного вывода о причастности необходимо установить не только принадлежность реквизита, но и лицо, которое фактически управляло цифровым инструментом в момент совершения значимых действий.

Теоретико-понятийная основа исследования состоит в разграничении четырёх уровней: киберпреступление как криминалистически значимое деяние; цифровой инструмент как средство совершения или сокрытия; цифровой след как отражение действия в электронной среде; фактический контроль как доказуемая связь лица с использованием соответствующего инструмента. Такое разграничение

создаёт методологическую основу для анализа практических способов доказывания фактического контроля.

Теоретическое разграничение цифрового следа, цифрового инструмента и фактического контроля приобретает практическое значение при оценке типичных источников доказательственной информации. В делах о киберпреступлениях исходный цифровой объект нередко указывает не на лицо, непосредственно управлявшее преступной схемой, а на технический или финансовый канал, через который совершалось действие. Поэтому установление владельца банковской карты, SIM-карты, аккаунта, IP-адреса, электронного кошелька или криптоадреса является начальным ориентиром расследования, но не завершает процесс доказывания.

Наиболее распространённая ситуация связана с банковскими картами и электронными платёжными инструментами, оформленными на одно лицо, но используемыми другим. Формальная принадлежность карты подтверждает регистрационную связь между банком и владельцем счёта, однако не раскрывает фактического пользователя банковского приложения, получателя SMS-кода, лица, инициировавшего перевод, снявшего наличные либо передавшего реквизиты третьим лицам. Банковская выписка должна оцениваться во взаимосвязи с устройством входа, временем авторизации, IP-данными, способом подтверждения операции, последующими переводами, обналичиванием и получением вознаграждения. Иначе факт поступления денежных средств на карту может быть ошибочно воспринят как достаточное подтверждение роли владельца карты в преступлении, хотя такое лицо может быть посредником, дропом, номинальным владельцем либо лицом, не осознававшим полного характера схемы [5].

Аналогичная проблема возникает при использовании SIM-карт. Регистрация номера на конкретного абонента сама по себе не доказывает, что именно он применял SIM-карту для совершения преступления. В киберпреступных схемах номер телефона может использоваться для регистрации аккаунта, получения одноразовых кодов, подтверждения банковских операций, восстановления доступа к сервису, связи с потерпевшим или привязки к электронному кошельку. При этом фактический контроль над SIM-картой может перейти к другому лицу без изменения регистрационных данных у оператора связи. Проверке подлежат не только анкетные сведения абонента, но и устройство, IMEI, период активности, география использования, замена или восстановление номера, связь с банковскими приложениями, аккаунтами и платежами. Без такой проверки номер телефона остаётся идентификатором канала связи, а не доказательством участия зарегистрированного владельца.

Отдельную группу трудностей образуют аккаунты в мессенджерах,

социальных сетях, маркетплейсах, платёжных сервисах и иных цифровых платформах. Аккаунт может быть создан на формальные данные одного лица, передан другому пользователю, продан, взломан, использоваться удалённо либо администрироваться несколькими участниками схемы. Следователь должен установить не только регистрационные данные аккаунта, но и историю входов, IP-адреса, привязанные номера, электронные адреса, изменение профиля, переписку, контакты, жалобы пользователей, связь с платёжными реквизитами и действия после совершения преступления. Скриншот переписки или ссылка на профиль имеют ориентирующее значение, но не заменяют проверки первичного источника, поскольку содержание аккаунта может быть изменено, удалено или имитировано.

Особую сложность создаёт дистанционное использование аккаунта. Внешне коммуникация с потерпевшим может исходить от конкретного профиля, но фактическое управление им может осуществляться с другого устройства, через удалённый доступ, VPN-сервис, прокси-соединение или ранее похищенные учётные данные. Поэтому сведения об аккаунте должны сопоставляться с данными платформы, устройством доступа, временными параметрами, финансовыми операциями и поведением пользователя [6]. Если такая проверка не проводится, расследование ограничивается внешним цифровым признаком и не обеспечивает установление лица, реально контролировавшего коммуникационный канал.

Криптоактивы усиливают указанную проблему, поскольку движение актива в блокчейн-среде может быть технически наблюдаемым, но не всегда персонализированным. Transaction hash позволяет установить факт операции, сеть, адрес отправителя и получателя, время, сумму и дальнейшее движение актива. Однако он не раскрывает личность лица, распорядившегося криптоактивом. Публичная проверяемость транзакции подтверждает цифровое событие, но не отвечает на вопрос о том, кто обладал приватным ключом, seed-фразой, логином, паролем, доступом к аппаратному кошельку или аккаунту криптобиржи. Следовательно, transaction hash должен проверяться в совокупности с данными устройства, криптобиржевого аккаунта, IP-адресов входа, KYC-профиля, переписки о передаче доступа, истории конвертации, источника приобретения актива и последующего распоряжения им [7].

Именно в этой части проявляется связь настоящей статьи с подготовленными автором научно-практическими предложениями к проекту постановления Пленума Верховного суда Республики Узбекистан. В разработанных предложениях обращено внимание на то, что передача криптоактива может осуществляться не только путём прямой транзакции, но и через сообщение адреса криптокошелька,

логина, пароля или seed-фразы. Данное положение не рассматривается в настоящей статье как действующее судебное разъяснение и не используется в качестве источника обязательного правового регулирования. Его значение состоит в практической апробации исследовательской идеи: при расследовании операций с криптоактивами доказыванию подлежит не только сам факт перемещения актива, но и наличие у конкретного лица средств фактического доступа и распоряжения.

Такой подход позволяет избежать смешения двух разных обстоятельств: технической фиксации операции и уголовно-процессуального доказывания участия лица. Криптокошелёк может быть связан с адресом, но распоряжение активом осуществляет тот, кто контролирует ключи доступа. Банковская карта может быть оформлена на одного гражданина, но управление мобильным приложением может находиться у другого. SIM-карта может быть зарегистрирована на формального абонента, но применяться участником схемы для подтверждения операций. Аккаунт может содержать данные одного пользователя, но фактически использоваться иным лицом. Поэтому практическая задача расследования состоит не в механическом закреплении регистрационной принадлежности, а в установлении реального управления цифровым инструментом в момент значимого действия.

Данная проблема проявляется и при оценке роли дропов. Лицо, предоставившее карту, счёт, SIM-карту, электронный кошелёк или доступ к аккаунту, может выполнять различные функции: номинального владельца, технического посредника, получателя перевода, участника вывода средств, лица, передающего доступ, либо осведомлённого звена организованной схемы. Один и тот же внешний признак – поступление денежных средств на карту – может иметь различное доказательственное значение в зависимости от того, знал ли владелец о преступном происхождении средств, передавал ли реквизиты, получал ли вознаграждение, участвовал ли в переводах, скрывал ли следы и взаимодействовал ли с организатором. Поэтому оценка роли лица должна вытекать из совокупности регистрационных, технических, поведенческих и финансовых данных, а не из одного факта оформления инструмента на его имя.

Практико-доказательственное значение рассматриваемой проблемы состоит в необходимости перехода от линейной модели **“реквизит – владелец – причастность”** к проверочной модели **“инструмент – доступ – действие – распоряжение – выгода”**. Такая модель требует последовательного установления: кто имел доступ к устройству; кто получал коды подтверждения; кто входил в аккаунт; кто менял настройки; кто инициировал платёж;

кто контролировал кошелёк; кто направлял дальнейшее движение средств; кто получил конечную имущественную выгоду. Только такая последовательность позволяет связать цифровой след с фактическим пользователем и исключить преждевременную персонализацию обвинительной версии [8].

Устранение методического риска, при котором формальный владелец цифрового или финансового инструмента автоматически воспринимается как фактический пользователь, требует самостоятельной методической модели проверки. Такая модель должна быть применима к банковским картам, SIM-картам, аккаунтам, электронным кошелькам, криптокошелькам, устройствам, IP-активности и иным цифровым объектам, используемым при совершении киберпреступлений. Её назначение состоит в переводе расследования от простой фиксации реквизита к установлению лица, реально управлявшего инструментом в момент юридически значимого цифрового действия.

Предлагаемая модель проверки фактического контроля строится на четырёх группах признаков: регистрационных, технических, поведенческих и финансово-транзакционных. Данные группы не образуют изолированных доказательственных блоков. Их значение проявляется только при сопоставлении, поскольку каждый признак в отдельности может иметь нейтральное, ориентирующее или ошибочно интерпретируемое значение. Регистрация карты, наличие SIM-карты, вход в аккаунт, IP-соединение, получение SMS-кода или криптоактивная транзакция должны оцениваться не как готовый вывод о причастности, а как элемент проверяемой доказательственной конструкции.

Первая группа – регистрационные признаки. К ним относятся сведения о лице, на имя которого оформлены банковская карта, банковский счёт, SIM-карта, аккаунт, электронный кошелёк, криптобиржевой профиль, домен, платёжный сервис или иной цифровой инструмент. Эти признаки позволяют определить первоначальную формальную связь между лицом и объектом, но не раскрывают характер фактического использования. Поэтому регистрационные сведения должны фиксироваться как отправная точка проверки, а не как самостоятельное основание для вывода о виновности. Их доказательственное значение повышается только тогда, когда они подтверждаются иными данными: устройством доступа, операционной активностью, перепиской, движением средств, поведением лица и получением имущественной выгоды.

Вторая группа – технические признаки. Она включает сведения об устройстве, IP-адресе, IMEI, IMSI, MAC-адресе, геолокации, времени подключения, логах входа, используемом браузере или приложении, пароле, PIN-коде, SMS-коде, push-подтверждении, электронной подписи, приватном ключе, seed-фразе и иных средствах

аутентификации. Данная группа имеет особое значение, поскольку позволяет перейти от формального реквизита к механизму доступа. Если карта оформлена на одно лицо, но вход в банковское приложение осуществлялся с устройства другого лица, это требует проверки фактического пользователя. Если аккаунт зарегистрирован на определённый номер, но входы выполнялись с другого устройства или из другой локации, регистрационная связь не может считаться достаточной. Если криптоактив перемещён с конкретного адреса, но данные указывают на использование seed-фразы или приватного ключа иным лицом, предметом доказывания становится не только транзакция, но и контроль над средствами доступа.

Третья группа – поведенческие признаки. К ним относятся переписка, голосовые сообщения, инструкции другим участникам, согласование переводов, поиск потерпевших, создание или размещение объявлений, удаление данных, переименование аккаунта, смена пароля, очистка истории, выход из профиля после операции, попытка блокировки доступа, объяснения лица, характер его контактов и действия после поступления денежных средств. Поведенческие признаки позволяют оценить не только техническую возможность использования инструмента, но и волевую связь лица с преступной схемой. Именно эта группа помогает разграничивать номинального владельца, неосведомлённого пользователя, технического посредника, дропа, непосредственного исполнителя и организатора.

Четвёртая группа – финансово-транзакционные признаки. В неё входят маршрут движения денежных средств, первый получатель, промежуточные переводы, повторяемость реквизитов, короткий интервал между поступлением и выводом средств, обналичивание, перевод на электронные кошельки, конвертация в криптоактивы, обмен через криптосервисы, последующий вывод, распределение средств между участниками и получение вознаграждения. Эта группа позволяет установить, кто фактически распоряжался преступным результатом. Поступление средств на карту или кошелёк само по себе не является достаточной основой для вывода о причастности владельца, но последующее распоряжение, согласованность переводов, регулярность операций и связь с другими участниками могут придать этим сведениям доказательственное значение.

Методическая ценность предложенной модели состоит в том, что она исключает линейную схему доказывания “инструмент – владелец – причастность”. Вместо неё предлагается последовательная проверочная схема: “инструмент – доступ – действие – распоряжение – выгода”. На первом этапе устанавливается, какой цифровой или финансовый инструмент использован. На втором этапе

выясняется, кто имел доступ к нему технически и фактически. На третьем этапе определяется, какие действия совершались через данный инструмент. На четвёртом этапе анализируется распоряжение результатом преступления. На пятом этапе проверяется наличие выгоды, координации либо иной связи с участниками схемы.

Для практического применения указанная модель может быть оформлена в виде матрицы фактического контроля. По каждому цифровому инструменту в такой матрице целесообразно фиксировать: формального владельца; предполагаемого фактического пользователя; источник сведений; признаки, подтверждающие контроль; признаки, опровергающие контроль; процессуальный способ получения информации; необходимость участия специалиста или назначения экспертизы; связь с другими инструментами; связь с иными лицами; уровень доказательственной подтверждённости. Такая матрица не заменяет процессуальную оценку доказательств, но дисциплинирует расследование и препятствует необоснованному отождествлению регистрационного владельца с фактическим пользователем.

Особое значение матрица приобретает при расследовании хищений через электронные платёжные системы и криптоактивы. В этих делах один и тот же участник может использовать несколько инструментов: SIM-карту для регистрации аккаунта, банковскую карту для получения средств, мессенджер для связи с потерпевшим, электронный кошелёк для промежуточного перевода, криптокошелёк для сокрытия финансового следа. При раздельной оценке каждый объект может выглядеть как самостоятельный цифровой эпизод. При матричной проверке выявляется связанная структура: кто обеспечивал доступ, кто управлял коммуникацией, кто принимал средства, кто выводил активы, кто координировал действия, и кто получил конечный результат.

В рамках предложенной модели криптоактивы требуют специального подхода. Transaction hash должен фиксироваться как техническое подтверждение движения актива, но не как доказательство личности распорядителя. Для установления фактического контроля необходимо проверять адрес кошелька, тип сети, время транзакции, аккаунт криптобиржи, KYC-данные, IP-адреса входа, устройство, seed-фразу, приватный ключ, логин, пароль, переписку о передаче доступа, историю обмена и последующее распоряжение активом [9]. В подготовленных автором научно-практических предложениях к проекту постановления Пленума Верховного суда Республики Узбекистан указано, что передача криптоактива может осуществляться не только прямой транзакцией, но и сообщением адреса криптокошелька, логина, пароля или seed-фразы. В настоящей статье это положение используется не как действующее судебное разъяснение, а как

практическая апробация более широкой криминалистической идеи: доказательственное значение имеет не только перемещение актива, но и контроль над средствами доступа к нему.

Важным условием применения модели является проверка как подтверждающих, так и опровергающих признаков фактического контроля. Следователь должен устанавливать не только обстоятельства, указывающие на связь лица с цифровым инструментом, но и данные, которые могут эту связь ослаблять или исключать. К ним относятся утрата карты, передача телефона другому лицу, дистанционный доступ, взлом аккаунта, использование публичной сети, техническая подмена IP-адреса, отсутствие доступа к SMS-кодам, невозможность физического использования устройства в конкретное время, отсутствие выгоды и несоответствие поведения лица роли активного участника. Такой подход соответствует требованиям объективности доказывания и снижает риск обвинительной интерпретации одного цифрового признака.

Предлагаемая модель также позволяет точнее разграничивать роли участников киберпреступной схемы. Формальный владелец карты или SIM-карты может быть потерпевшим, неосведомлённым владельцем, дропом, посредником, техническим участником или соисполнителем. Разграничение этих ролей невозможно только по регистрационным сведениям. Оно требует проверки осведомлённости, характера передачи доступа, вознаграждения, повторности действий, участия в переписке, связи с организатором, последующего распоряжения средствами и поведения после совершения операции. Поэтому модель фактического контроля имеет значение не только для установления лица, но и для правильной оценки его процессуального положения и роли в расследуемом событии.

С процессуальной точки зрения применение модели должно быть связано с законным получением и закреплением электронных данных. Сведения об аккаунтах, устройствах, банковских операциях, телекоммуникационных соединениях, криптоактивных транзакциях и электронных сообщениях должны включаться в доказывание через предусмотренные законом процессуальные формы [10]. Законодательное закрепление цифровых доказательств в Республике Узбекистан усиливает значение этой задачи, поскольку электронные данные должны оцениваться с учётом источника происхождения, способа получения, целостности, относимости, допустимости и достоверности. Методика фактического контроля не отменяет эти требования, а определяет, какие именно обстоятельства должны быть проверены для связи цифрового следа с конкретным лицом.

Следовательно, авторское решение заключается в признании фактического контроля над

цифровым инструментом самостоятельным криминалистическим критерием проверки по делам о киберпреступлениях. Его нельзя понимать как новую презумпцию виновности или замену уголовно-процессуального доказывания. Напротив, данная категория направлена на повышение качества доказывания, поскольку требует установить не только формальную принадлежность карты, номера, аккаунта или кошелька, но и реальную возможность лица использовать этот инструмент, совершить через него значимое действие, распорядиться результатом и получить выгоду.

Проведённый анализ позволяет сформулировать основной вывод: при расследовании киберпреступлений доказыванию подлежит не только наличие цифрового следа, но и фактический контроль конкретного лица над цифровым инструментом, посредством которого совершено действие, обеспечен доступ, подтверждена операция, переданы данные либо осуществлено распоряжение преступным результатом. Цифровой след фиксирует электронное событие, однако не всегда раскрывает субъекта, управлявшего соответствующим устройством, аккаунтом, картой, SIM-картой, электронным кошельком или криптоактивом.

Формальная принадлежность цифрового инструмента имеет ориентирующее, но не окончательное доказательственное значение. Регистрация банковской карты, номера телефона, аккаунта или кошелька указывает на первоначальную связь лица с соответствующим объектом, но не подтверждает автоматически его участие в преступлении. Такая связь должна проверяться через совокупность регистрационных, технических, поведенческих и финансово-транзакционных признаков. Только их согласованная оценка позволяет установить, кто фактически использовал инструмент, обладал средствами доступа, инициировал цифровое действие, контролировал движение средств и получил либо обеспечил получение выгоды.

Предлагаемая категория фактического контроля не создаёт презумпцию причастности лица к преступлению. Её назначение состоит в противоположном: исключить необоснованное отождествление владельца реквизита с фактическим пользователем и обеспечить проверку как подтверждающих, так и опровергающих обстоятельств. Поэтому в делах о киберпреступлениях следственная версия должна строиться не вокруг формального статуса владельца карты, номера, аккаунта или криптокошелька, а вокруг доказуемой связи лица с доступом, действием, распоряжением и результатом.

Особое значение данный подход имеет при расследовании операций с криптоактивами. Transaction hash подтверждает факт движения актива в соответствующей сети, но не устанавливает лицо,

распорядившееся им. Для субъектной привязки криптооперации необходимо проверять адрес кошелька, приватный ключ, seed-фразу, логин, пароль, аккаунт криптобиржи, IP-адреса входа, устройство, KYC-данные, переписку о передаче доступа и последующее распоряжение активом. В этом проявляется различие между технической наблюдаемостью транзакции и уголовно-процессуальным доказыванием участия конкретного лица.

Авторские научно-практические предложения к проекту постановления Пленума Верховного суда Республики Узбекистан использованы в статье как форма апробации подхода к доказыванию контроля над криптоактивами, без придания им значения действующего судебного разъяснения.

Методическое значение статьи заключается в обосновании проверочной модели “инструмент – доступ – действие – распоряжение – выгода”. Эта модель позволяет системно оценивать цифровую информацию, не ограничиваясь её внешним содержанием. Она ориентирует следователя на установление источника электронных данных, законности их получения, технической целостности, связи с событием и связи с конкретным лицом. В таком виде цифровое доказательство приобретает не только информационную, но и процессуальную устойчивость.

Фактический контроль над цифровым инструментом следует рассматривать как самостоятельный криминалистический критерий проверки по делам о киберпреступлениях. Его установление позволяет преодолеть разрыв между цифровым следом и доказательственным выводом о лице, участвовавшем в преступной схеме. Для практики расследования это означает необходимость закрепления алгоритма, при котором банковские, телекоммуникационные, платформенные, экспертные и криптоактивные данные оцениваются в единой системе, направленной на установление реального пользователя цифрового инструмента.

References:

1. Уголовно-процессуальный кодекс Республики Узбекистан: утв. Законом Республики Узбекистан от 22 сентября 1994 г. № 2013-XII. – Ст. 204^1, 204^2 // Национальная база данных законодательства Республики Узбекистан. – URL: https://lex.uz/acts/111463 (дата обращения: 10.06.2026); Закон Республики Узбекистан “О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами” от 21 ноября 2024 г. № ЗРУ-1003 // Национальная база данных законодательства Республики Узбекистан. – URL: https://lex.uz/ru/docs/7228823 (дата обращения: 12.06.2026).

2. Ҳуқуқни муҳофаза қилиш академияси томонидан ахборот технологиялари соҳасидаги экспертиза фаолиятининг долзарб муаммолари, компьютер-техник экспертизанинг назарий ва амалий жиҳатлари юзасидан ўтказилган тадқиқот натижалари бўйича Бош прокуратурага киритилган таҳлилий маълумотнома. – Тошкент, 2025. – Б. 1.

3. См.: Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений: дис. … канд. юрид. наук: 12.00.12. – М., 2016. – С. 15-38; Завьялова Д. В. Расследование преступлений в сфере компьютерной информации: отечественный и зарубежный опыт: дис. … канд. юрид. наук: 12.00.12. – М., 2021. – С. 17-37; Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования: монография / под науч. ред. Е. В. Смахтина, Р. Д. Шарапова, В. И. Морозова. – Тюмень : Изд-во Тюменского государственного университета, 2021. – С. 22-35, 266-295.

4. Convention on Cybercrime : ETS No. 185. Budapest, 23 November 2001 // Council of Europe Treaty Office. – URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 (дата обращения: 15.06.2026).

5. Коновалов И., Йўлдошев Т., Арипов А. Ўзбекистон Республикасида жиноий мақсадларда банк ҳисобварақларини тақдим этиш ва улардан фойдаланишга қарши курашишнинг жиноят-ҳуқуқий механизмларини такомиллаштириш: илмий рисола. – Тошкент: Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси, Рақамли криминалистика илмий-тадқиқот институти, 2025. – Б. 9-18, 54-60.

6. Practical Guide for Requesting Electronic Evidence Across Borders / United Nations Office on Drugs and Crime, Counter-Terrorism Committee Executive Directorate, International Association of Prosecutors. – Vienna, 2019 // UNODC SHERLOC. – URL: https://www.unodc.org/cld/en/publications/practical-guide/practical-guide.html (дата обращения: 17.06.2026); Common Challenges in Cybercrime / Eurojust, Europol. – The Hague, 2024. – URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Common_Challenges_in_Cybercrime_2024.pdf (дата обращения: 19.06.2026).

7. Рақамли криминалистика: дарслик / Г. Ф. Мусаев, Г. М. Гаджиев, Б. Б. Кудратов [ва бошқ.]. – Тошкент: Ўзбекистон Республикаси Ҳуқуқни муҳофаза қилиш академияси, Рақамли криминалистика илмий-тадқиқот институти, 2025. – Б. 156-168.

8. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: CETS No. 224. Strasbourg, 12 May 2022 // Council of Europe Treaty Office. – URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224 (дата обращения: 20.06.2026).

9. FATF. Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets. – Paris : FATF, 2020. – URL: https://www.fatf-

gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf.coredownload.pdf (дата обращения: 22.06.2026).

10. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response: NIST Special Publication 800-86. – Gaithersburg: National Institute of Standards and Technology, 2006. – DOI: 10.6028/NIST.SP.800-86. – URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (дата обращения: 25.06.2026).