European Journal of Interdisciplinary Research and Development
Volume- 52 June- 2026
Website: www.ejird.journalspark.org ISSN (E): 2720-5746

ОБЪЕКТИВНЫЕ И СУБЪЕКТИВНЫЕ ПРИЗНАКИ КИБЕРМОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: УГОЛОВНО-ПРАВОВОЙ И СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ

Саттаров Джасурбек Авазбекович,
Самостоятельный соискатель Правоохранительной академии Республики Узбекистан
E-mail: jasur_sattarov@proacademy.uz

Аннотация

В статье исследуются объективные и субъективные признаки мошенничества, совершаемого с использованием информационных технологий, в контексте уголовного законодательства Республики Узбекистан, современной уголовно-правовой доктрины, судебной практики и сравнительно-правовых подходов. Обосновывается, что цифровизация имущественного оборота изменила не только технический способ совершения мошенничества, но и сам механизм преступного воздействия на волю потерпевшего, форму имущественного вреда, структуру причинной связи и способы доказывания умысла. Особое внимание уделяется фишингу, вишингу, смишингу, онлайн-кредитованию, мобильному банкингу, QR-кодовым платежам, электронным кошелькам, Telegram-ботам, поддельным аккаунтам и иным цифровым инструментам, используемым для завладения чужим имуществом или имущественным правом. На основе анализа законодательства Узбекистана, Германии, Великобритании, США, Казахстана, России, Будапештской конвенции и Конвенции ООН против киберпреступности формулируется авторский вывод о необходимости комплексной оценки объективной и субъективной стороны кибермошенничества. Предлагаются авторские определения кибермошенничества, цифрового введения в заблуждение, объективной и субъективной стороны данного преступления, а также рекомендации по совершенствованию разъяснений Пленума Верховного суда Республики Узбекистан и методики оценки цифровых доказательств.

Ключевые слова: кибермошенничество, информационные технологии, цифровая среда, объективная сторона, субъективная сторона, прямой умысел, корыстная цель, цифровое введение в заблуждение, фишинг, вишинг, смишинг, онлайн-кредитование, электронные платёжные средства.

Introduction
Введение

Современная цифровая трансформация финансового оборота, банковских услуг, электронных платежей, онлайн-кредитования, дистанционной идентификации и социальных коммуникаций существенно изменила криминологический и уголовно-правовой облик мошенничества. Если в классической модели мошенничества обман

чаще всего реализовывался посредством личного контакта, устного обещания, письменного документа, фиктивной сделки или злоупотребления ранее сложившимися доверительными отношениями, то в цифровой среде преступное воздействие всё чаще осуществляется через интерфейс мобильного приложения, электронное сообщение, поддельную ссылку, QR-код, бот, фальшивый аккаунт, виртуальную карту, онлайн-кредитный сервис или систему электронных платежей.

В уголовном законодательстве Республики Узбекистан мошенничество традиционно определяется как завладение чужим имуществом или правом на чужое имущество путём обмана или злоупотребления доверием. Вместе с тем совершение такого деяния с использованием информационных систем, в том числе информационных технологий, выступает квалифицирующим признаком, что придаёт данной форме посягательства повышенную общественную опасность [1].

Существенное значение для правоприменения имеет постановление Пленума Верховного суда Республики Узбекистан от 23 июня 2023 года № 17 «О судебной практике по делам о мошенничестве». В нём мошенничество раскрывается через воздействие обмана или злоупотребления доверием на волю собственника, иного владельца имущества, его представителя либо уполномоченного органа, в результате чего имущество или право на него передаются виновному либо создаётся возможность для их изъятия [2]. В указанном постановлении также разъясняется момент окончания мошенничества: оно считается оконченным с момента поступления имущества в незаконное владение виновного или иных лиц и получения ими реальной возможности пользоваться либо распоряжаться им.

Однако цифровая среда порождает ряд вопросов, которые не могут быть решены путём простого перенесения традиционных подходов к мошенничеству. Во-первых, необходимо определить, является ли информационная технология лишь техническим средством совершения преступления либо она способна трансформировать структуру объективной стороны состава. Во-вторых, требуется установить, как в условиях онлайн-коммуникации проявляются обман и злоупотребление доверием. Во-третьих, особую сложность представляет доказывание субъективной стороны: прямого умысла, корыстной цели, заранее сформированного намерения завладеть чужим имуществом или имущественным правом. В-четвёртых, возникает вопрос разграничения кибермошенничества, гражданско-правового спора, компьютерного правонарушения, неправомерного доступа к информации и иных смежных составов.

Цель настоящей статьи состоит в формировании комплексной уголовно-правовой характеристики кибермошенничества, совершаемого с использованием информационных технологий, через взаимосвязанный анализ его объективных и субъективных признаков. Для достижения этой цели необходимо: раскрыть уголовно-правовую природу цифрового способа совершения мошенничества; определить значение информационных технологий в механизме преступления; выявить особенности объективной стороны; проанализировать субъективную сторону и проблему доказывания прямого умысла; сопоставить подходы законодательства

Узбекистана с зарубежными и международно-правовыми моделями; выработать предложения по совершенствованию законодательства и судебной практики.

Методологическую основу исследования составляют формально-юридический, сравнительно-правовой, системно-структурный, доктринальный и уголовно-правовой методы, а также метод правового моделирования и анализа судебной практики. Особое значение имеет системный подход, поскольку кибермошенничество не может быть адекватно понято только как «мошенничество через интернет». Оно представляет собой сложную форму имущественного посягательства, в которой психологическое воздействие на потерпевшего соединяется с технической манипуляцией цифровой инфраструктурой.

Цифровизация имущественного оборота привела к тому, что традиционные признаки мошенничества стали проявляться в иной фактической и доказательственной среде. В классической модели мошенничества центральное значение имеет искажённое представление потерпевшего о фактах, правах, намерениях или возможностях виновного. Потерпевший, находясь под влиянием обмана либо злоупотребления доверием, сам передаёт имущество, предоставляет доступ к нему либо создаёт условия для перехода имущественного права к виновному. В цифровой модели этот психологический механизм сохраняется, однако опосредуется технологическим интерфейсом.

Именно поэтому кибермошенничество нельзя сводить только к использованию компьютера, смартфона или сети Интернет. Информационная технология в подобных преступлениях выполняет как минимум три функции. Первая коммуникативная: с её помощью виновный доводит ложную информацию до потерпевшего. Вторая манипулятивная: цифровая среда используется для создания искусственного доверия, например через поддельный сайт банка, фальшивый аккаунт государственного органа или интерфейс, имитирующий официальный платёжный сервис. Третья имущественно-трансакционная: именно через цифровую систему происходит перевод денежных средств, оформление онлайн-кредита, создание виртуальной карты, подтверждение платежа или изменение имущественного положения потерпевшего.

В этом смысле информационные технологии становятся не внешним техническим фоном, а элементом преступного механизма. Справедливо отмечал Ю.М. Батурин, что компьютерная преступность не всегда создаёт абсолютно новые преступления; чаще она модифицирует традиционные посягательства под воздействием технологической среды [3]. Однако такая модификация не является поверхностной. Она затрагивает форму обмана, способ причинения вреда, момент окончания преступления и структуру доказывания.

Схожую мысль развивает У. Зибер, рассматривая киберпреступность как явление, в котором компьютерные технологии выступают одновременно объектом, средством и средой преступной деятельности [4]. Данный подход особенно важен для анализа кибермошенничества. В одних случаях цифровая технология используется только как канал сообщения ложной информации: например, SMS с фальшивым уведомлением о блокировке карты. В других случаях технология является инструментом

преобразования имущественного состояния: например, когда посредством онлайн-сервиса оформляется кредит на потерпевшего, создаётся виртуальная карта, после чего средства переводятся на счета виновного или связанных с ним лиц.

Поэтому авторская позиция состоит в том, что кибермошенничество, совершаемое с использованием информационных технологий, следует рассматривать как технологически опосредованную форму имущественного посягательства, при которой обман или злоупотребление доверием реализуются через цифровые каналы коммуникации, цифровые средства идентификации, электронные платёжные инструменты либо вмешательство в результат обработки информации, а конечной целью выступает незаконное получение имущественной выгоды.

Такой подход позволяет избежать двух методологических крайностей. Первая крайность заключается в чрезмерном расширении понятия кибермошенничества, когда любое нарушение договорного обязательства в онлайн-среде ошибочно квалифицируется как преступление. Вторая крайность, напротив, состоит в недооценке цифрового способа, когда информационные технологии рассматриваются только как нейтральный инструмент, не влияющий на структуру объективной и субъективной стороны. Обе позиции являются неполными. Цифровой способ не отменяет классических признаков мошенничества, но придаёт им новую форму проявления.

В уголовно-правовой теории объективная сторона преступления традиционно рассматривается как совокупность внешних признаков общественно опасного деяния, включающих действие или бездействие, общественно опасные последствия, причинную связь, способ, место, время, обстановку, орудия и средства совершения преступления [5]. Л.Д. Гаухман подчёркивал, что объективная сторона выражает внешнюю социально значимую сторону преступного посягательства, позволяющую установить его фактическую форму и степень общественной опасности [6]. В.Н. Кудрявцев, развивая проблему причинной связи и механизма преступного поведения, указывал, что уголовно-правовая оценка невозможна без анализа того, каким образом деяние привело к общественно опасному результату [7].

Применительно к кибермошенничеству объективная сторона имеет усложнённую структуру. Она включает не только традиционное сообщение ложных сведений либо сокрытие фактов, но и создание цифровой ситуации доверия, формирование ложного интерфейса, использование электронных платёжных средств, манипулирование цифровыми идентификаторами, а также трансакционное перемещение имущественной ценности. Поэтому объектом анализа становится не отдельное сообщение виновного, а вся последовательность действий: создание ложного цифрового образа, вовлечение потерпевшего в доверительную коммуникацию, получение от него данных или согласия, запуск платёжной либо кредитной операции, переход имущества или имущественного права под контроль виновного.

В условиях цифровой среды обман может выражаться в нескольких формах. Во-первых, это сообщение заведомо ложной информации через электронные каналы: SMS, мессенджеры, электронную почту, голосовой звонок, push-уведомление, поддельную ссылку. Во-вторых, это создание ложного визуального или функционального образа:

фальшивый сайт банка, копия интерфейса платёжной организации, имитация официального Telegram-бота, поддельный личный кабинет. В-третьих, это использование чужого статуса или репутации: представление сотрудником банка, оператором платёжной системы, представителем государственного органа, службы безопасности или онлайн-площадки. В-четвёртых, это сокрытие существенных обстоятельств, которые виновный обязан был раскрыть, например факта оформления кредита на имя потерпевшего или направления платежа не по назначению.

Пленум Верховного суда Республики Узбекистан справедливо исходит из того, что обман при мошенничестве может выражаться не только в сообщении ложных сведений, но и в умолчании об обстоятельствах, имеющих значение для волеизъявления потерпевшего [8]. В цифровой среде такое умолчание приобретает особую специфику. Потерпевший нередко не видит реального получателя платежа, не понимает технического значения SMS-кода, не осознаёт, что вводимые данные используются не для «защиты карты», а для доступа к мобильному банкингу или оформления кредитного обязательства. Виновный, используя технологическую асимметрию, сознательно скрывает истинное назначение операции.

Злоупотребление доверием также получает цифровую форму. Если ранее оно чаще было связано с личными, семейными, служебными или деловыми отношениями, то теперь всё чаще основано на институциональном доверии к цифровой инфраструктуре. Потерпевший доверяет не столько конкретному лицу, сколько символам официальности: логотипу банка, доменному имени, оформлению сайта, названию канала, интерфейсу приложения, номеру телефона, похожему на официальный. В этом смысле цифровая среда позволяет виновному искусственно конструировать доверие без реальной социальной связи с потерпевшим.

Особую сложность представляет вопрос о действии и бездействии. Базовая модель кибермошенничества чаще всего предполагает активное поведение: рассылку ложных сообщений, создание поддельного сайта, запуск бота, звонок потерпевшему, изменение QR-кода, получение SMS-кода, оформление онлайн-кредита, перевод денежных средств. Однако в ряде случаев активное действие соединяется с умолчанием. Например, виновный убеждает потерпевшего в необходимости «проверки безопасности», но скрывает, что фактически получает доступ к его банковскому приложению. Либо сообщает, что операция является отменой платежа, хотя в действительности она подтверждает перевод средств. Следовательно, объективная сторона кибермошенничества нередко имеет смешанную структуру: активное цифровое воздействие дополняется сокрытием юридически значимых фактов.

Имущественный вред при кибермошенничестве также не всегда выражается в прямом изъятии наличных или безналичных денежных средств. Он может проявляться в незаконном возникновении кредитного обязательства, списании средств с электронного кошелька, переводе средств на подконтрольную карту, утрате контроля над аккаунтом, получении имущественного права, создании обязательства по возврату займа или микрокредита. Поэтому уголовно-правовое понимание вреда должно охватывать не только фактическое уменьшение имущества потерпевшего, но и

ухудшение его имущественного положения вследствие незаконно созданной обязанности.

В этом контексте момент окончания преступления следует определять не формально, а функционально. Если денежные средства поступили на счёт виновного или третьего лица, находящегося под его контролем, и появилась реальная возможность распоряжения ими, мошенничество следует признавать оконченным. Если же через онлайн-кредитование на потерпевшего незаконно возложено долговое обязательство, а кредитные средства направлены в цифровой контур, контролируемый виновным, окончание преступления должно связываться не только с физическим получением денег, но и с возникновением имущественно неблагоприятного правового состояния потерпевшего. Иной подход искусственно сужал бы содержание имущественного вреда в цифровой экономике.

Авторское определение объективной стороны кибермошенничества можно сформулировать следующим образом: объективная сторона мошенничества, совершаемого с использованием информационных технологий, представляет собой внешне выраженную систему действий или сочетание действий и умолчания, посредством которых виновный через цифровые средства коммуникации, идентификации, обработки данных либо электронных платежей вводит потерпевшего, информационную систему или уполномоченный цифровой сервис в заблуждение, создаёт условия для перехода имущества или имущественного права и причиняет имущественный вред либо создаёт незаконное имущественное обременение.

Если объективная сторона показывает внешнюю форму преступления, то субъективная сторона раскрывает внутреннее психическое отношение виновного к совершаемому деянию и его последствиям. В уголовно-правовой доктрине субъективная сторона традиционно включает вину, мотив, цель и эмоциональное состояние лица. При этом вина является обязательным признаком состава преступления, а мотив и цель имеют значение в тех случаях, когда они прямо предусмотрены законом или вытекают из юридической природы состава [9].

Применительно к мошенничеству центральным признаком является прямой умысел. Лицо осознаёт, что сообщает ложные сведения, скрывает истинные факты или злоупотребляет доверием; понимает, что в результате этого чужое имущество или имущественное право перейдёт к нему либо другому лицу; желает наступления такого результата. Н.Ф. Кузнецова подчёркивала, что субъективная сторона преступления не может быть сведена к формальному признанию вины, поскольку именно через внутреннее отношение лица определяется социальная и правовая природа содеянного [10]. А.И. Рарог, анализируя субъективную сторону преступления, указывал, что умысел должен устанавливаться не изолированно, а через совокупность обстоятельств деяния, поведения виновного до, во время и после совершения преступления [11].

Эти положения имеют принципиальное значение для кибермошенничества. Сам факт использования информационной технологии не доказывает мошеннический умысел. Ошибка в онлайн-сделке, технический сбой, невозможность своевременно исполнить

договор, спор о качестве услуги или задержка поставки товара не образуют состава мошенничества, если отсутствовало заранее сформированное намерение завладеть чужим имуществом путём обмана. Поэтому квалификация должна строиться не на результате как таковом, а на установлении преступного замысла в момент получения имущества, данных, доступа или цифрового согласия.

В цифровой среде прямой умысел проявляется через последовательность подготовительных и исполнительских действий. К таким признакам могут относиться: создание поддельного аккаунта; использование чужого имени, бренда или логотипа; массовая рассылка однотипных сообщений; подготовка фальшивого сайта; изменение платёжного QR-кода; использование анонимных карт или электронных кошельков; быстрое распределение поступивших средств между несколькими счетами; удаление переписки; применение VPN, подставных номеров, ботов и иных средств сокрытия следов. Каждый из этих признаков сам по себе не всегда достаточен для вывода о мошенничестве, но их совокупность способна свидетельствовать о заранее сформированном умысле.

Корыстная цель также является обязательным элементом мошенничества. Однако в условиях цифровой экономики её нельзя понимать исключительно как стремление получить наличные деньги. Корыстная цель в цифровой среде может быть направлена на получение доступа к банковскому счёту, оформление онлайн-кредита на потерпевшего, перевод средств на электронный кошелёк, приобретение имущественного права, получение цифрового актива, захват аккаунта, использование персональных данных для последующего извлечения имущественной выгоды. Следовательно, корыстная цель кибермошенничества должна пониматься как направленность виновного на незаконное получение имущественной выгоды посредством установления контроля над цифровым ресурсом, имущественным правом, платёжным инструментом или финансовым обязательством.

Необходимо разграничивать мотив и цель. Мотив отвечает на вопрос, почему лицо совершает преступление; цель какого результата оно стремится достичь. Мотивом может быть желание быстрого обогащения, погашения долга, поддержания преступной схемы, участия в группе, получения статуса в криминальной среде. Целью же выступает конкретный противоправный результат: получить деньги, оформить кредит, завладеть доступом к мобильному банкингу, изменить направление платежа, вывести средства через электронный кошелёк. В цифровой среде это различие особенно важно, поскольку цель нередко имеет многоэтапный технический характер.

Авторское определение субъективной стороны кибермошенничества может быть выражено следующим образом: субъективная сторона мошенничества, совершаемого с использованием информационных технологий, представляет собой прямой, заранее сформированный и корыстно ориентированный умысел лица, осознающего ложный либо манипулятивный характер цифрового воздействия, предвидящего переход имущества, имущественного права или имущественного контроля к себе либо третьему лицу и желающего наступления такого результата.

Сложность доказывания субъективной стороны заключается в том, что внутреннее отношение лица не наблюдается непосредственно. Оно устанавливается через внешние цифровые следы: переписку, скриншоты, историю входов, IP-адреса, транзакции, данные мобильного оператора, сведения платёжных систем, логи приложений, запись телефонных разговоров, последовательность переводов, удаление аккаунтов и повторяемость действий. В этой связи цифровые доказательства приобретают не только техническое, но и уголовно-правовое значение: они позволяют реконструировать не только факт операции, но и преступный сценарий.

Квалификация мошенничества, совершаемого с использованием информационных технологий, не может быть построена исключительно на анализе внешнего поведения виновного либо только на установлении его внутреннего отношения к содеянному. В цифровой среде объективная и субъективная стороны преступления находятся в более тесной взаимосвязи, чем в классических формах имущественных посягательств. Это объясняется тем, что цифровой способ совершения преступления, как правило, заранее проектируется виновным, требует подготовки технической инфраструктуры, моделирования поведения потерпевшего и расчёта последовательности имущественной операции.

Так, создание поддельного сайта банка, фальшивого Telegram-бота, QR-кода, ведущего на иной платёжный счёт, либо аккаунта, имитирующего официальное лицо, одновременно имеет двойное юридическое значение. С одной стороны, эти действия характеризуют объективную сторону преступления, поскольку являются внешним способом введения потерпевшего в заблуждение. С другой стороны, они указывают на субъективную сторону, так как свидетельствуют о предварительном формировании умысла, осознании ложного характера создаваемой цифровой ситуации и стремлении получить имущественную выгоду.

Именно поэтому при квалификации кибермошенничества нельзя ограничиваться вопросом о том, был ли использован телефон, компьютер, мессенджер или банковское приложение. Юридически значимым является не сам факт применения технологии, а её функция в преступном механизме. Если информационная технология выступает лишь случайным каналом общения между сторонами гражданско-правового отношения, то этого недостаточно для вывода о мошенничестве. Однако если цифровая технология используется для создания ложной доверительной среды, получения доступа к имущественным ресурсам, сокрытия реального назначения операции или трансформации имущественного положения потерпевшего, она становится квалификационно значимым элементом преступной схемы.

Такой подход соответствует позиции Пленума Верховного суда Республики Узбекистан, согласно которой мошенничество предполагает воздействие обмана или злоупотребления доверием на волю лица, в результате чего имущество или право на него переходит к виновному либо создаётся возможность для такого перехода. Постановление Пленума от 23 июня 2023 года № 17 также подчёркивает значение момента фактического получения возможности пользоваться или распоряжаться имуществом. В цифровой среде это разъяснение должно применяться с учётом

специфики безналичных платежей, онлайн-кредитования, виртуальных карт и электронных кошельков.

В доктринальном плане здесь необходимо отказаться от изолированного анализа признаков состава. Объективная сторона показывает, каким образом виновный сконструировал ложную цифровую реальность; субъективная сторона отвечает на вопрос, осознавал ли он её ложный характер и желал ли наступления имущественного результата. Например, если лицо направляет потерпевшему ссылку, визуально имитирующую официальный сайт банка, получает через неё данные карты и затем переводит средства на подконтрольный счёт, то объективно имеет место цифровое введение в заблуждение и имущественное перемещение, а субъективно прямой корыстный умысел. Эти признаки не существуют раздельно, а взаимно подтверждают друг друга.

В этой связи целесообразно предложить следующий квалификационный тест для установления кибермошенничества:

создана ли виновным ложная цифровая ситуация, влияющая на волю потерпевшего или результат обработки информации;

использовалась ли информационная технология не случайно, а как элемент механизма обмана, злоупотребления доверием или имущественного перемещения;

возникло ли в результате этого имущественное последствие утрата средств, незаконное возникновение обязательства, переход имущественного права или получение контроля над платёжным инструментом;

подтверждается ли цифровыми следами заранее сформированный умысел виновного на получение имущественной выгоды;

имеется ли причинная связь между цифровым обманом, действиями потерпевшего или информационной системы и наступившим имущественным результатом.

Данный тест позволяет разграничить кибермошенничество и смежные ситуации. Например, обычное неисполнение онлайн-договора не образует мошенничества, если отсутствует заранее сформированный умысел на завладение имуществом. Техническая ошибка платёжной системы не является мошенничеством, если лицо не создавало ложной ситуации и не стремилось получить выгоду. Напротив, если лицо изначально создаёт фиктивный цифровой образ, заведомо не намерено исполнять обязательство, использует однотипную схему в отношении многих потерпевших и быстро выводит полученные средства, совокупность этих обстоятельств указывает на преступный характер поведения.

Сравнительно-правовой анализ показывает, что государства используют различные модели уголовно-правового реагирования на мошенничество в цифровой среде. Условно можно выделить три подхода: технологически нейтральный, специальный компьютерно-правовой и смешанный.

Германское уголовное законодательство представляет один из наиболее показательных примеров специального регулирования компьютерного мошенничества. Наряду с классическим мошенничеством, закреплённым в § 263 Уголовного кодекса Германии, § 263a предусматривает самостоятельный состав компьютерного мошенничества. Его

сущность заключается в причинении имущественного вреда путём воздействия на результат обработки данных: неправильного программирования, использования неверных или неполных данных, несанкционированного использования данных либо иного неправомерного влияния на процесс обработки информации. Официальный перевод StGB указывает, что § 263a направлен на случаи, когда имущественный вред причиняется через воздействие на результат обработки данных при намерении получить незаконную имущественную выгоду.

Германский подход ценен тем, что он позволяет охватить случаи, когда обман направлен не непосредственно на человека, а на информационную систему. В классическом мошенничестве ключевым элементом является введение человека в заблуждение, тогда как компьютерное мошенничество предполагает манипуляцию процессом обработки данных. Это важно для тех цифровых схем, где потерпевший может вообще не принимать активного решения о передаче имущества, а имущественный результат возникает вследствие вмешательства в систему.

Для Узбекистана германская модель представляет значительный научный интерес, однако её механическое заимствование не представляется необходимым. Действующая конструкция статьи 168 УК Республики Узбекистан уже позволяет квалифицировать многие цифровые формы мошенничества через признак использования информационных систем и информационных технологий. Вместе с тем германский опыт показывает, что в национальных разъяснениях следует отдельно раскрыть случаи, когда мошеннический результат достигается не только через психологическое воздействие на потерпевшего, но и через неправомерное влияние на результат цифровой обработки данных.

Великобритания избрала иной путь. Fraud Act 2006 не создаёт отдельного состава «кибермошенничества», а формулирует технологически нейтральную модель мошенничества. Закон выделяет мошенничество путём ложного представления, путём нераскрытия информации и путём злоупотребления положением; при этом ложное представление признаётся преступным, если оно сделано нечестно и с намерением получить выгоду либо причинить другому лицу ущерб или риск ущерба.

Сильная сторона британского подхода заключается в его гибкости. Он не привязывает мошенничество к конкретной технологии, что позволяет применять нормы к новым цифровым схемам без постоянного изменения уголовного закона. Фишинг, смишинг, вишинг, поддельные инвестиционные платформы, онлайн-объявления и QR-кодовые схемы могут охватываться общей конструкцией ложного представления, если доказаны нечестность и намерение получить выгоду или причинить ущерб.

Для Узбекистана этот подход полезен прежде всего с точки зрения законодательной техники. Вместо излишнего дробления составов возможно сохранить общую норму о мошенничестве, но дать более точные судебные разъяснения о том, как цифровые формы обмана вписываются в традиционные признаки состава. При этом британская модель демонстрирует особую значимость субъективного критерия dishonest intent, то есть нечестного намерения, направленного на получение выгоды или причинение убытка.

Американское право использует многоуровневую модель, в которой цифровое мошенничество может охватываться нормами о wire fraud, computer fraud, access device fraud, identity fraud и рядом иных федеральных составов. Особый интерес представляет 18 U.S.C. § 1030, предусматривающий ответственность за мошенничество и связанную деятельность в отношении компьютеров. В частности, § 1030(a)(4) охватывает случаи, когда лицо, действуя сознательно и с намерением обмануть, получает несанкционированный доступ к защищённому компьютеру либо превышает разрешённый доступ и посредством такого поведения получает нечто ценное.

Американская модель подчёркивает два важных признака: неправомерный доступ или превышение полномочий и намерение обмануть. Это отличает компьютерное мошенничество от обычного нарушения правил пользования системой. Для квалификации требуется не просто техническое нарушение, а его связь с мошеннической целью и получением ценности.

Для Узбекистана данный подход может быть полезен при разграничении кибермошенничества и преступлений против информационной безопасности. Если лицо получает доступ к системе без цели имущественного обогащения, речь может идти о неправомерном доступе или ином компьютерном правонарушении. Если же доступ используется для получения денег, имущественного права, кредита, цифрового актива или иной ценности, уголовно-правовой центр тяжести смещается к мошенничеству.

Казахстанское уголовное законодательство сохраняет традиционное понимание мошенничества как хищения чужого имущества или приобретения права на чужое имущество путём обмана или злоупотребления доверием. Статья 190 УК Республики Казахстан формулирует мошенничество именно через эти признаки.

Казахстанский опыт близок узбекской модели, поскольку обе системы исходят из классической конструкции мошенничества, дополняемой квалифицирующими обстоятельствами и судебными разъяснениями. Практическая ценность данного подхода состоит в том, что цифровые формы мошенничества не отрываются от общей природы имущественного посягательства. Вместе с тем сохраняется риск недостаточной конкретизации цифровых схем, если судебная практика не выработает единые критерии оценки онлайн-кредитования, электронных платежей, фишинга и манипуляций с цифровыми идентификаторами.

Российское законодательство пошло по пути выделения специального состава мошенничества в сфере компьютерной информации. Статья 159.6 УК РФ предусматривает ответственность за хищение чужого имущества или приобретение права на чужое имущество путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации. Такая модель конкретизирует объективную сторону компьютерного мошенничества, однако одновременно порождает вопросы разграничения с общим мошенничеством, неправомерным доступом и иными преступлениями в сфере компьютерной информации.

Для Узбекистана российская модель представляет интерес, но её полное заимствование не является бесспорным. Создание отдельной статьи о компьютерном мошенничестве может усилить определённость закона, однако способно усложнить квалификацию и привести к конкуренции норм. Более рациональным представляется сохранение общей статьи о мошенничестве при одновременном уточнении содержания квалифицирующего признака «с использованием информационных технологий» и разработке разъяснений по типовым цифровым схемам.

Будапештская конвенция о киберпреступности в статье 8 предусматривает компьютерно-связанное мошенничество, связанное с причинением имущественного ущерба путём ввода, изменения, удаления или подавления компьютерных данных либо иного вмешательства в функционирование компьютерной системы, когда деяние совершается умышленно и неправомерно. Конвенция также допускает требование специального мошеннического или аналогичного нечестного умысла.

Конвенция ООН против киберпреступности, принятая Генеральной Ассамблеей ООН в 2024 году, закрепляет в статье 13 обязанность государств криминализировать кражу или мошенничество, связанные с информационно-коммуникационными системами, когда имущественный вред причиняется посредством ввода, изменения, удаления, подавления электронных данных, вмешательства в функционирование ИКТ-системы либо введения лица в заблуждение относительно фактических обстоятельств через такую систему.

Обе конвенционные модели имеют принципиальное значение для Узбекистана. Они подтверждают, что современное кибермошенничество может проявляться в двух формах: как цифровое введение человека в заблуждение и как воздействие на результат обработки данных. Следовательно, национальная уголовно-правовая политика должна учитывать обе модели, не сводя кибермошенничество исключительно к онлайн-обману потерпевшего.

Практическое значение исследования кибермошенничества особенно ярко проявляется в вопросах доказывания. В традиционном мошенничестве следствие и суд, как правило, исследуют показания потерпевшего, свидетелей, договоры, расписки, движение денежных средств, характер обещаний виновного и его последующее поведение. В цифровой среде к этому добавляется значительный массив электронных доказательств: переписки, скриншоты, IP-адреса, данные мобильных операторов, логи банковских приложений, сведения о транзакциях, истории входов, метаданные файлов, электронные чеки, записи звонков, сведения о владельцах аккаунтов и цифровых кошельков.

Главная проблема состоит в том, что цифровое доказательство должно подтверждать не только факт технической операции, но и уголовно-правовое содержание поведения. Например, сам по себе перевод денег на карту ещё не доказывает мошенничества. Необходимо установить, почему потерпевший совершил перевод, какие сведения ему были сообщены, понимал ли он реальное назначение операции, кто контролировал аккаунт или номер телефона, как быстро были выведены средства, повторялась ли

схема в отношении других лиц, предпринимал ли виновный действия по сокрытию следов.

Особую сложность представляет доказывание прямого умысла. В цифровой среде виновный редко прямо признаёт, что изначально намеревался похитить деньги. Поэтому умысел устанавливается через систему косвенных признаков. К ним относятся: использование ложного имени или статуса; создание интерфейса, сходного с официальным; применение заранее подготовленного сценария общения; массовость сообщений; получение одноразовых кодов; оформление кредитов на третьих лиц; мгновенное распределение средств по нескольким картам; удаление переписки; использование подставных номеров; отсутствие реальной возможности исполнить обещанное обязательство; многократное повторение аналогичных эпизодов.

Важное значение имеет разграничение кибермошенничества и гражданско-правового спора. Постановление Пленума Верховного суда Республики Узбекистан № 17 исходит из того, что при отсутствии признаков преступления споры, вытекающие из договорных отношений, должны разрешаться в гражданско-правовом порядке. Данный подход имеет особую актуальность для онлайн-торговли, дистанционных услуг и электронной коммерции. Неисполнение договора, задержка поставки, спор о качестве товара или невозможность возврата долга не должны автоматически криминализироваться. Уголовно-правовая оценка допустима только тогда, когда будет доказано, что уже в момент получения имущества виновный не намеревался исполнять обязательство и использовал цифровой обман как средство завладения чужими средствами.

При онлайн-кредитовании момент возникновения умысла и момент причинения вреда требуют особенно внимательного анализа. Потерпевший может не передавать виновному деньги непосредственно. Однако если виновный получает его персональные данные, оформляет на него кредит, переводит средства на виртуальную карту и затем выводит их на подконтрольный счёт, имущественный вред выражается не только в движении денежных средств, но и в незаконном возложении долгового обязательства на потерпевшего. Следовательно, оценка ущерба должна учитывать как фактическое перемещение денег, так и возникновение неблагоприятного имущественно-правового состояния.

В делах о фишинге, вишинге и смишинге ключевое значение имеет установление причинной связи между ложным цифровым воздействием и имущественным результатом. Потерпевший вводит данные карты, сообщает SMS-код или переходит по ссылке именно потому, что находится в заблуждении относительно характера операции. Если это заблуждение создано виновным, а последующее списание средств является прямым результатом такого воздействия, причинная связь должна признаваться установленной.

Особое место занимает оценка поведения виновного после получения средств. В доктрине справедливо указывается, что последующее неисполнение обязательства само по себе не доказывает первоначального мошеннического умысла. Однако если последующее поведение согласуется с заранее созданной цифровой схемой быстрый

вывод средств, блокировка потерпевшего, удаление аккаунта, смена номера, использование поддельных реквизитов, повторение аналогичных действий, оно приобретает значение косвенного доказательства первоначального умысла.

Таким образом, цифровые доказательства должны оцениваться не фрагментарно, а в виде единой доказательственной цепочки: создание ложной цифровой среды контакт с потерпевшим получение данных или согласия совершение имущественной операции вывод средств сокрытие следов последующее поведение виновного. Только такая модель позволяет избежать как необоснованной криминализации гражданско-правовых отношений, так и недооценки опасных цифровых мошеннических схем.

Проведённый анализ позволяет сформулировать ряд предложений, направленных на повышение эффективности уголовно-правового противодействия кибермошенничеству в Республике Узбекистан.

Во-первых, целесообразно дополнить постановление Пленума Верховного суда Республики Узбекистан от 23 июня 2023 года № 17 отдельным пунктом, посвящённым мошенничеству, совершаемому с использованием информационных технологий. В этом пункте следует разъяснить, что под использованием информационных технологий при мошенничестве понимается не только применение компьютера, но и использование смартфона, мобильного приложения, электронного кошелька, банковской карты, виртуальной карты, QR-кода, аккаунта, мессенджера, бота, поддельного сайта, цифрового идентификатора или онлайн-платформы для введения лица в заблуждение либо создания условий для перехода имущества или имущественного права.

Во-вторых, в разъяснениях Пленума необходимо закрепить критерии установления прямого умысла в цифровой среде. К таким критериям могут быть отнесены: создание поддельного цифрового образа; использование ложного статуса; массовая рассылка сообщений; подготовка фиктивных интерфейсов; сокрытие реального получателя платежа; использование чужих персональных данных; быстрое перечисление средств на иные счета; удаление электронных следов; повторяемость схемы; отсутствие реальной возможности исполнить обещанное обязательство.

В-третьих, необходимо специально разъяснить вопросы онлайн-кредитования. Следует указать, что если виновный путём обмана или злоупотребления доверием оформляет кредит, микрозайм, рассрочку или иной финансовый продукт на имя потерпевшего, а полученные средства переводит под свой контроль либо контроль третьих лиц, имущественный вред выражается не только в списании денежных средств, но и в незаконном возложении финансового обязательства на потерпевшего.

В-четвёртых, необходимо разработать межведомственную методику выявления, фиксации и оценки цифровых доказательств по делам о кибермошенничестве. Такая методика должна охватывать порядок получения данных от банков, платёжных организаций, мобильных операторов, интернет-провайдеров, владельцев платформ и администраторов мессенджеров; правила фиксации скриншотов и переписок; проверку подлинности электронных следов; восстановление транзакционной цепочки; установление фактического контролёра аккаунта, карты или электронного кошелька.

В-пятых, следует уточнить научно-практическое понимание момента окончания кибермошенничества. При безналичных операциях преступление должно признаваться оконченным с момента поступления средств на счёт, карту, электронный кошелёк или иной цифровой инструмент, находящийся под контролем виновного или связанных с ним лиц, если появилась реальная возможность распоряжения средствами. При онлайн-кредитовании окончание может связываться также с незаконным возникновением имущественного обязательства потерпевшего и переходом кредитных средств в цифровой контур, контролируемый виновным.

В-шестых, в учебно-методических материалах для следователей, прокуроров и судей целесообразно закрепить типологию кибермошенничества. Она может включать: фишинговую модель; вишинговую модель; смишинговую модель; модель онлайн-кредитного мошенничества; модель манипуляции QR-кодом; модель злоупотребления электронными платёжными средствами; модель поддельной инвестиционной платформы; модель мошенничества через маркетплейсы и социальные сети; смешанную модель социальной инженерии и технической манипуляции.

В-седьмых, при совершенствовании законодательства необходимо соблюдать баланс между технологической конкретизацией и стабильностью уголовно-правовой нормы. Излишне детальное перечисление технологий может быстро устареть. Поэтому предпочтительно использовать обобщающие формулы: «информационная система», «информационно-коммуникационная технология», «электронное платёжное средство», «цифровой идентификатор», «онлайн-платформа», «электронный финансовый сервис». Их содержание может быть раскрыто в судебных разъяснениях и специальных методических рекомендациях.

Заключение

Кибермошенничество, совершаемое с использованием информационных технологий, представляет собой не просто традиционное мошенничество, перенесённое в интернет-пространство, а сложную форму имущественного посягательства, в которой психологическое воздействие на потерпевшего соединяется с технологической манипуляцией цифровой инфраструктурой. Информационные технологии в подобных преступлениях выполняют не только роль средства связи, но и функцию создания доверительной иллюзии, получения доступа к имущественным ресурсам, сокрытия истинного назначения операции и трансформации имущественного положения потерпевшего.

Объективная сторона кибермошенничества выражается в системе действий или действий, соединённых с умолчанием, посредством которых виновный через цифровые каналы коммуникации, электронные платёжные инструменты, онлайн-платформы, мобильные приложения, QR-коды, боты или иные технологические средства вводит потерпевшего либо цифровую систему в заблуждение и добивается перехода имущества, имущественного права или имущественного контроля. При этом имущественный вред может выражаться не только в прямом списании средств, но и в

незаконном возникновении кредитного обязательства, утрате контроля над платёжным инструментом или создании имущественно неблагоприятного правового состояния.

Субъективная сторона данного преступления характеризуется прямым, заранее сформированным и корыстно ориентированным умыслом. Виновный осознаёт ложный или манипулятивный характер цифрового воздействия, предвидит переход имущества или имущественного контроля и желает наступления такого результата. Корыстная цель в цифровой среде должна пониматься широко как стремление получить незаконную имущественную выгоду посредством цифрового доступа, платёжного инструмента, электронного кошелька, онлайн-кредита, персональных данных или иной имущественно значимой цифровой возможности.

Сравнительно-правовой анализ показывает, что зарубежные модели предлагают различные варианты регулирования: германская система выделяет компьютерное мошенничество как специальный состав; британская модель использует технологически нейтральную конструкцию; американское право сочетает нормы о компьютерном доступе, wire fraud и получении ценности; казахстанский подход близок узбекской общей модели мошенничества; российское право выделяет мошенничество в сфере компьютерной информации. Международные стандарты, закреплённые в Будапештской конвенции и Конвенции ООН против киберпреступности 2024 года, подтверждают необходимость охвата как цифрового введения человека в заблуждение, так и неправомерного воздействия на результат обработки данных.

Для законодательства и судебной практики Узбекистана наиболее рациональным представляется не механическое создание отдельной статьи о компьютерном мошенничестве, а функциональное развитие действующей конструкции статьи 168 УК через уточнение квалифицирующего признака использования информационных технологий, дополнение разъяснений Пленума Верховного суда и разработку методики оценки цифровых доказательств. Такой подход позволит сохранить системность уголовного закона, избежать конкуренции норм и одновременно обеспечить адекватную правовую оценку современных цифровых мошеннических схем.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Уголовный кодекс Республики Узбекистан. Национальная база данных законодательства Республики Узбекистан. Ст. 168.
2. Постановление Пленума Верховного суда Республики Узбекистан от 23 июня 2023 г. № 17 «О судебной практике по делам о мошенничестве».
3. Батурин Ю.М. Проблемы компьютерного права. М.: Юридическая литература, 1991.
4. Гаухман Л.Д. Квалификация преступлений: закон, теория, практика. М.: Центр ЮрИнфоР, 2005.
5. Уголовное право: учебное пособие / под ред. Л.Д. Гаухмана, С.В. Максимова. М.: Элит, 2007.
6. Уголовное право. Общая часть: учебник / под ред. Н.И. Ветрова, Ю.И. Ляпунова. М.: Юриспруденция, 2007.

7. Кудрявцев В.Н. Объективная сторона преступления. М.: Госюриздат, 1960.
8. Кузнецова Н.Ф. Преступление и преступность. М.: Издательство Московского университета, 1969.
9. Наумов А.В. Российское уголовное право. Общая часть: курс лекций. М.: БЕК, 1996.
10. Рарог А.И. Субъективная сторона преступления. М.: Проспект, 2019.
11. Жалинский А.Э. Современное немецкое уголовное право. М.: Проспект, 2004.
12. Волженкин Б.В. Мошенничество. СПб.: Юридический центр Пресс, 2002.
13. Бойцов А.И. Преступления против собственности. СПб.: Юридический центр Пресс, 2002.
14. Комиссаров В.С. Преступления в сфере компьютерной информации: вопросы квалификации. М.: Юрлитинформ, 2003.
15. Очилов Ҳ.Р. Ўзгалар мулкини компьютер воситаларидан фойдаланиб талон-торож қилганлик учун жавобгарлик: юрид. фан. бўйича фалсафа доктори (PhD) дисс. Тошкент, 2017.
16. Алтиев Р.С. Фирибгарликнинг жиноят-ҳуқуқий ва криминологик жиҳатлари: юрид. фан. бўйича фалсафа доктори (PhD) дисс. Тошкент, 2020.
17. Абдурасулова Қ.П. Фирибгарликнинг жиноят-ҳуқуқий муаммолари: юрид. фан. номз. дисс. Тошкент, 1996.
18. Rustambayev M.H. O‘zbekiston Respublikasi jinoyat huquqi kursi. 1-tom. Toshkent, 2018.
19. Sieber U. The International Handbook of Computer Crime: Computer-Related Economic Crime and the Infringements of Privacy. Chichester: John Wiley & Sons, 1986.
20. Gercke M. Understanding Cybercrime: Phenomena, Challenges and Legal Response. Geneva: International Telecommunication Union, 2012.
21. Clough J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2015.
22. Brenner S.W. Cybercrime: Criminal Threats from Cyberspace. Santa Barbara: Praeger, 2010.
23. Kerr O.S. Computer Crime Law. St. Paul: West Academic Publishing, 2013.
24. Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press, 2007.
25. Yar M. Cybercrime and Society. London: SAGE Publications, 2013.
26. Levi M. The Phantom Capitalists: The Organization and Control of Long-Firm Fraud. Aldershot: Ashgate, 2008.
27. Grabosky P. Electronic Crime. Upper Saddle River: Prentice Hall, 2007.
28. Šepec M. Slovenian Criminal Code and Modern Criminal Law Approach to Computer-Related Fraud: A Comparative Legal Analysis // International Journal of Cyber Criminology. 2012.
29. German Criminal Code (Strafgesetzbuch, StGB). §§ 263, 263a. Federal Ministry of Justice.
30. Fraud Act 2006. United Kingdom Public General Acts. Sections 1–5.
31. 18 U.S.C. § 1030. Fraud and related activity in connection with computers.

32. Criminal Code of the Republic of Kazakhstan. Article 190.
33. Уголовный кодекс Российской Федерации. Ст. 159.6.
34. Convention on Cybercrime. Budapest, 23 November 2001. Council of Europe. Article 8.
35. United Nations Convention against Cybercrime. 2024. Article 13.