ЦИФРОВОЕ МОШЕННИЧЕСТВО КАК ОСОБЫЙ ВИД МОШЕННИЧЕСТВА

Латифа Валиева
Ведущий научный сотрудник Института законодательства и правовой политики при Президенте Республики Узбекистан

АННОТАЦИЯ

В статье рассматривается цифровое мошенничество как результат трансформации традиционного мошенничества под воздействием цифровизации имущественного оборота. Анализируются особенности объекта и предмета посягательства, способы противоправного завладения имуществом в цифровой среде, механизм причинения имущественного ущерба и содержание умысла виновного. Критически оцениваются положения статей 167 и 168 Уголовного кодекса Республики Узбекистан с точки зрения их применимости к современным схемам хищения, совершаемым посредством информационных систем, цифровых платформ, средств удаленного доступа и приемов социальной инженерии. Обосновывается необходимость законодательного закрепления понятия цифрового мошенничества и уточнения квалифицирующих признаков мошенничества, совершаемого с использованием информационно-коммуникационных технологий.

Ключевые слова: *мошенничество, цифровое мошенничество, хищение, информационные технологии, информационная система, социальная инженерия, электронные денежные средства, уголовная ответственность.*

ABSTRACT

The article examines digital fraud as a result of the transformation of traditional fraud under the influence of the digitalization of property relations and economic transactions. It analyzes the specific features of the object and subject matter of the criminal encroachment, the methods of unlawful appropriation of property in the digital environment, the mechanism through which pecuniary damage is caused, and the content of the offender's intent. Articles 167 and 168 of the Criminal Code of the Republic of Uzbekistan are critically assessed in terms of their applicability to contemporary forms of property appropriation committed through information systems, digital platforms, remote-access tools, and social engineering techniques. The article substantiates the need to introduce a statutory definition of digital fraud and to clarify the qualifying circumstances applicable to fraud committed through information and communication technologies.

Keywords: *fraud, digital fraud, misappropriation of property, information technologies, information system, social engineering, electronic money, criminal liability.*

Цифровизация общественных отношений качественно изменила не только формы экономического оборота, но и механизм совершения преступлений против собственности. Денежные средства, имущественные права и юридически значимая информация все чаще существуют, передаются и подтверждаются посредством банковских приложений, информационных систем, цифровых платформ и средств электронной идентификации. Вследствие этого мошенничество постепенно утрачивает исключительно традиционную форму непосредственного обмана потерпевшего и приобретает признаки технологически организованного дистанционного посягательства.

Действующая статья 168 Уголовного кодекса Республики Узбекистан определяет мошенничество как завладение чужим имуществом или правом на чужое имущество путем обмана или злоупотребления доверием.[1] Пунктом «в» части третьей данной статьи отдельно предусмотрено совершение мошенничества с использованием информационной системы, в том числе информационных технологий.[1] Такое дополнение свидетельствует о признании законодателем повышенной общественной опасности технологически опосредованного мошенничества. Вместе с тем существующая конструкция не разрешает всех вопросов квалификации современных цифровых схем.

В научной литературе для обозначения рассматриваемых деяний используются понятия «кибермошенничество», «дистанционное мошенничество», «компьютерное мошенничество» и «цифровое мошенничество». Эти категории не являются полностью тождественными. Понятие киберпреступности охватывает широкий круг посягательств, направленных не только против собственности, но и против безопасности информационных систем, конфиденциальности данных и устойчивости цифровой инфраструктуры. Дистанционность характеризует отсутствие непосредственного физического контакта между виновным и потерпевшим, однако не раскрывает технологическую природу преступления [4; 7]. Компьютерное мошенничество, напротив, может быть понято слишком узко – как деяние, связанное преимущественно с воздействием на компьютерную информацию.

Наиболее содержательным представляется понятие цифрового мошенничества, поскольку оно охватывает хищения, при которых информационно-коммуникационные технологии используются для создания обмана, воздействия на волю потерпевшего, получения доступа к имуществу, осуществления транзакции, сокрытия личности виновного либо легализации преступного результата. В исследовании Д.М. Ибатуллиной информационные технологии предлагается рассматривать не как самостоятельный способ хищения, а как средство реализации мошеннического умысла, позволяющее установить контакт с потерпевшим, расширить круг потенциальных жертв и обеспечить удаленное завладение имуществом [4]. Данный подход заслуживает поддержки, но требует уточнения применительно к различным механизмам цифрового посягательства.

Цифровое мошенничество сохраняет основной объект традиционного мошенничества – общественные отношения собственности. Однако цифровая форма деяния нередко затрагивает также отношения, обеспечивающие безопасность использования персональных данных, банковской информации, средств аутентификации и информационных систем. Эти отношения не во всех случаях образуют самостоятельный дополнительный объект преступления. Например, направление потерпевшему ложного сообщения от имени банка нарушает установленный порядок безопасного информационного взаимодействия, но основная направленность умысла виновного заключается в завладении денежными средствами. Иная ситуация возникает при неправомерном проникновении в информационную систему, блокировании или изменении данных: в таких случаях наряду с собственностью может непосредственно нарушаться информационная безопасность, что ставит вопрос о квалификации содеянного по совокупности преступлений.

Специфика цифрового мошенничества проявляется и в предмете посягательства. Им могут выступать наличные и безналичные денежные средства, электронные деньги, денежные средства на банковских счетах, имущественные права, цифровые финансовые активы, права требования, учетные записи, подарочные сертификаты и иные объекты, обладающие экономической ценностью. Вместе с тем персональные данные, пароль, код подтверждения, реквизиты банковской карты или ключ доступа сами по себе не всегда являются предметом хищения. В большинстве случаев они выступают средством получения контроля над имуществом либо промежуточным объектом противоправного воздействия.

Поэтому цифровая природа мошенничества определяется не только нематериальной формой имущества. Если лицо посредством социальной сети размещает объявление о продаже несуществующего товара и получает от потерпевшего обычный банковский перевод, предметом преступления остаются денежные средства. Цифровой характер деяния обусловлен механизмом формирования и реализации обмана: созданием ложного цифрового образа продавца, использованием платформы для поиска потерпевшего, дистанционным сообщением недостоверной информации и получением денежных средств через электронную платежную инфраструктуру.

Особенностью цифрового мошенничества является сочетание юридического способа хищения с техническими приемами его реализации. Юридически обязательным способом мошенничества остаются обман или злоупотребление доверием. Фишинговые сайты, подмена телефонных номеров, вредоносные ссылки, ложные аккаунты, программы удаленного доступа, поддельные платежные страницы и технологии синтеза голоса являются не самостоятельными формами хищения, а инструментами, посредством которых создается или поддерживается заблуждение потерпевшего.

Однако не каждое цифровое завладение имуществом образует мошенничество. Для мошенничества принципиально, что потерпевший либо иное уполномоченное лицо под влиянием обмана совершает юридически или фактически значимое действие: переводит денежные средства, сообщает сведения для доступа, подтверждает операцию, передает имущество либо предоставляет право на него. Если же денежные средства списываются без волеизъявления потерпевшего посредством непосредственного технического вмешательства в информационную систему, конструкция обмана как способа добровольной передачи имущества становится менее очевидной.

Пленум Верховного суда Республики Узбекистан разъясняет, что мошенничество с использованием информационной системы может совершаться посредством изменения информации, обрабатываемой или хранящейся в компьютерной системе, а также путем введения в систему ложной информации. Такое толкование расширяет сферу действия статьи 168 УК [2]. Вместе с тем оно частично сближает мошенничество с деяниями, при которых имущество изымается вследствие манипулирования информационной системой, а не вследствие введения человека в заблуждение.

Представляется, что разграничение должно осуществляться в зависимости от механизма перехода имущества. Если имущество передается самим потерпевшим или уполномоченным лицом под влиянием ложной информации,

содеянное соответствует классической конструкции мошенничества. Если виновный вводит ложные данные в автоматизированную систему и решение о перечислении средств принимается системой без непосредственного волеизъявления человека, такое деяние образует особую разновидность цифрового хищения. Его отнесение к мошенничеству возможно только при прямом указании закона, поскольку информационная система не обладает сознанием и не может быть обманута в уголовно-правовом смысле.

Субъективная сторона цифрового мошенничества характеризуется прямым умыслом и корыстной целью. Виновный осознает ложность сообщаемой информации либо противоправный характер цифрового воздействия, предвидит переход чужого имущества под свой контроль и желает наступления данного результата. При этом содержание умысла охватывает не только завладение имуществом, но и функциональное назначение применяемых технологий.

Например, лицо, создающее копию банковского сайта, должно понимать, что этот ресурс предназначен для введения пользователей в заблуждение и получения их платежных данных. Участник преступной группы, предоставляющий банковскую карту для зачисления похищенных средств, подлежит ответственности за соучастие в мошенничестве только тогда, когда установлено, что он осознавал преступный характер операций и желал содействовать завладению чужим имуществом. Сам факт предоставления карты или абонентского номера без доказывания осведомленности о мошеннической схеме недостаточен для вывода о наличии совместного умысла.

Для цифрового мошенничества характерна возможность поэтапного формирования преступного результата. Один участник создает техническую инфраструктуру, другой вступает в контакт с потерпевшим, третий принимает денежные средства, четвертый обналичивает или переводит их через цепочку счетов. В связи с этим при квалификации необходимо устанавливать интеллектуальный и волевой элементы умысла каждого участника, а не автоматически вменять всем лицам весь объем действий преступной группы.

Критического анализа требует соотношение статьи 168 УК со статьей 167 УК Республики Узбекистан [1]. Статья 167 предусматривает ответственность за присвоение или растрату чужого имущества, вверенного виновному либо находящегося в его ведении. В качестве особо квалифицирующего обстоятельства пункт «г» части третьей статьи называет использование средств компьютерной техники. Следовательно, применение данной нормы предполагает наличие двух обязательных условий: имущество первоначально находилось у виновного на законном основании и было ему вверено либо

находилось в его ведении; компьютерная техника использовалась при последующем противоправном обращении данного имущества.

Поэтому статья 167 УК не предназначена для квалификации большинства распространенных схем цифрового мошенничества. Денежные средства потерпевшего, полученные посредством фишинга, ложного интернет-магазина, телефонного обмана или поддельного инвестиционного сервиса, до совершения преступления не были вверены виновному. Их переход осуществляется именно вследствие обмана, что соответствует статье 168 УК. Пункт «г» части третьей статьи 167 применим преимущественно к ситуациям, когда работник банка, бухгалтер, оператор информационной системы или иное лицо, имеющее законный доступ к вверенному имуществу, использует компьютерную технику для его присвоения или растраты [1].

Формулировка «с использованием средств компьютерной техники» в статье 167 УК представляется устаревшей. Она ориентирована на материальное устройство – компьютер и его технические компоненты, тогда как современное цифровое хищение может совершаться посредством облачного сервиса, мобильного приложения, автоматизированного программного интерфейса, распределенной информационной системы или похищенных средств цифровой идентификации. Кроме того, само использование компьютера может не повышать общественную опасность присвоения: например, составление фиктивного электронного документа на служебном компьютере технически соответствует данной формулировке, хотя компьютер не играет определяющей роли в механизме хищения.

Более современной является конструкция пункта «в» части третьей статьи 168 УК, содержащая указание на информационную систему и информационные технологии. Однако она также имеет недостатки. Во-первых, термин «с использованием» обладает чрезмерно широким содержанием. Практически любое современное мошенничество может включать телефонный звонок, электронную переписку или перевод денежных средств через банковское приложение. Формальное применение квалифицирующего признака ко всем таким случаям способно необоснованно уравнять простое использование средства связи и сложное технологически организованное вмешательство в цифровую инфраструктуру.

Во-вторых, действующая норма не разграничивает использование информационных технологий как обычного средства коммуникации и их функциональное применение для создания ложной цифровой идентичности, автоматизированного воздействия на неопределенный круг лиц, получения

несанкционированного доступа либо манипулирования информацией. В-третьих, статья 168 УК не содержит легального определения цифрового мошенничества и не устанавливает четких критериев его отграничения от кражи, присвоения, неправомерного доступа к компьютерной информации и причинения имущественного ущерба путем обмана.

Необходимость дальнейшего совершенствования законодательства согласуется и с целями Стратегии кибербезопасности Республики Узбекистан на 2026–2030 годы, предусматривающей повышение эффективности предупреждения преступлений в сфере информационных технологий, развитие цифровой криминалистики и проведение исследований правовых аспектов противодействия современным киберпреступлениям [3].

Представляется целесообразным закрепить в примечании к статье 168 УК следующее определение:

«Цифровым мошенничеством признается завладение чужим имуществом или приобретение права на чужое имущество путем обмана либо злоупотребления доверием, при котором информационно-коммуникационные технологии, информационные системы, электронные сети или средства цифровой идентификации используются для формирования или поддержания заблуждения потерпевшего, получения доступа к имуществу либо обеспечения его противоправного перехода к виновному или другим лицам».

Предложенное определение сохраняет обязательную связь цифрового мошенничества с обманом или злоупотреблением доверием и одновременно раскрывает функциональную роль технологий. Простое использование телефона или компьютера, не имеющее существенного значения для механизма хищения, не должно автоматически образовывать квалифицированный состав.

Пункт «в» части третьей статьи 168 УК целесообразно изложить более конкретно: «с использованием информационно-коммуникационных технологий, информационных систем или средств цифровой идентификации, существенно облегчивших совершение преступления, обеспечивших дистанционное воздействие на потерпевшего, автоматизированное распространение обмана либо неправомерный доступ к его имуществу».

Дополнительными квалифицирующими признаками цифрового мошенничества могут быть признаны: совершение деяния посредством неправомерного использования персональных или аутентификационных данных; создание поддельного цифрового ресурса либо цифровой идентичности; применение средств автоматизации для воздействия на множество потерпевших; совершение преступления организованной группой с

распределением технических и финансовых функций; использование технологий искусственного интеллекта для имитации личности другого лица.

Одновременно формулировку пункта «г» части третьей статьи 167 УК целесообразно заменить указанием на использование информационной системы или информационно-коммуникационных технологий, если их применение обеспечило доступ к вверенному имуществу, изменение сведений о нем либо сокрытие его противоправного обращения. Это позволит связать квалифицирующий признак не с фактом наличия компьютера, а с его существенной ролью в механизме присвоения или растраты.

Таким образом, цифровое мошенничество представляет собой не только традиционный обман, перенесенный в электронную среду. Его специфика выражается в цифровом механизме формирования заблуждения, удаленном управлении поведением потерпевшего, использовании электронных средств доступа к имуществу, высокой масштабируемости и возможности распределения преступных функций между несколькими лицами. Статья 168 УК Республики Узбекистан в целом позволяет квалифицировать значительную часть подобных деяний, однако широкая формулировка признака использования информационных технологий не обеспечивает необходимой определенности. Статья 167 УК применима лишь к случаям противоправного обращения имущества, ранее вверенного виновному, и не может рассматриваться как общая норма о цифровом хищении.

Закрепление легального определения цифрового мошенничества, уточнение функциональной роли информационных технологий и разграничение обмана человека и манипулирования автоматизированной системой позволят повысить определенность уголовного закона и обеспечить единообразную квалификацию современных цифровых способов противоправного завладения имуществом.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Уголовный кодекс Республики Узбекистан от 22 сентября 1994 года № 2012-XII, статьи 167, 168.
2. Постановление Пленума Верховного суда Республики Узбекистан от 23 июня 2023 года № 17 «О судебной практике по делам о мошенничестве».
3. Указ Президента Республики Узбекистан от 10 марта 2026 года № УП-38 «Об определении Стратегии кибербезопасности Республики Узбекистан и совершенствовании системы предупреждения киберпреступности».
4. Ибатуллина Д.М. Объективные признаки цифрового мошенничества и их значение для квалификации деяния // Вестник Казанского юридического

института МВД России. 2025. Т. 16. № 1 (59). С. 66–73. DOI: 10.37973/VESTNIKKUI-2025-59-7.

5. Овсюков Д.А. Корыстные преступления против собственности с использованием информационно-телекоммуникационных сетей: вопросы квалификации: дис. … канд. юрид. наук. Москва, 2023. 231 с.

6. Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. д-ра юрид. наук. Москва, 2021. 521 с.

7. Зотина Е.В. Мошенничество с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии: криминологическое исследование: дис. канд. юрид. наук. Казань, 2024. 249 с.

8. Сергеев А.Ю., Широкова О.В. Мошенничество в цифровом обществе в условиях социальных изменений // Цифровая социология. 2023. № 1. С. 59–71.