ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ПЛАТЕЖНЫХ ИНСТРУМЕНТОВ

Шохайдарова Рисолахон Бехзод қизи
магистрант Ташкентского государственного юридического университета
https://doi.org/10.5281/zenodo.21988708

Аннотация. *В тезисе рассматриваются проблемы уголовно-правовой квалификации мошенничества, совершаемого с использованием банковских карт, мобильных приложений, электронных денег и иных цифровых платежных инструментов. Основное внимание уделено разграничению мошенничества и кражи в ситуациях, когда платеж формально подтвержден владельцем, но его воля сформирована под воздействием обмана, социальной инженерии либо вредоносного программного обеспечения. Проблематика раскрывается на основе законодательства Республики Узбекистан, официальной статистики и зарубежного опыта Европейского союза, Великобритании и США.*

Ключевые слова: *экономические преступления, мошенничество, цифровые платежи, банковская карта, информационная система, информационные технологии, социальная инженерия, квалификация.*

Цифровизация платежного оборота изменила не только способы совершения имущественных преступлений, но и сам механизм завладения денежными средствами. Если при традиционном мошенничестве обман непосредственно предшествует передаче имущества потерпевшим, то в цифровой среде между волеизъявлением лица и фактическим списанием средств находятся банковское приложение, идентификационные данные, одноразовый код, удаленный доступ к устройству и автоматизированные платежные операции. В результате один и тот же внешне похожий эпизод может содержать признаки как мошенничества, так и кражи либо иных преступлений, связанных с неправомерным воздействием на информационную систему. Для правоприменения ключевым становится вопрос: когда цифровая операция является результатом обманно сформированной воли потерпевшего, а когда имущество фактически изымается без его волевого участия.

Действующее уголовное законодательство Республики Узбекистан учитывает технологический способ совершения мошенничества. Согласно пункту «в» части третьей статьи 168 Уголовного кодекса Республики Узбекистан мошенничество, совершенное с использованием информационной системы, в том числе информационных технологий, образует квалифицированный состав преступления. Данная редакция действует с учетом изменений, внесенных Законом Республики Узбекистан от 22 июня 2026 года № ЗРУ-1155. Одновременно само понятие мошенничества в части первой статьи 168 УК по-прежнему строится на классической конструкции завладения чужим имуществом или правом на него путем обмана либо злоупотребления доверием. Следовательно, использование цифровой технологии само по себе не устраняет необходимости установить именно обманный способ завладения имуществом.

Особое значение имеет пункт 22 постановления Пленума Верховного суда Республики Узбекистан от 23 июня 2023 года № 17 «О судебной практике по делам о

мошенничестве». В нем разъясняется, что мошенничество с использованием информационных технологий может выражаться в изменении информации, обрабатываемой или хранящейся в компьютерной системе, либо во введении ложной информации в такую систему. При разграничении данного состава и кражи Пленум исходит из волевого критерия: при мошенничестве потерпевший в результате обмана или злоупотребления доверием добровольно передает имущество и осознает, что оно выбывает из его владения; при несанкционированном проникновении в информационную систему и изъятии имущества без такого волеизъявления речь идет о краже. При этом в тексте постановления Пленума сохраняется ссылка на прежний пункт «г» части третьей статьи 168 УК, тогда как после изменений от 22 июня 2026 года соответствующий квалифицирующий признак закреплен в пункте «в». Эта редакционная несогласованность сама по себе не меняет содержания разъяснения, однако наглядно показывает динамичность уголовно-правового регулирования цифровых форм хищения.

Наиболее сложная квалификационная ситуация возникает при применении социальной инженерии. Потерпевший может самостоятельно назвать злоумышленнику SMS-код, перейти по ссылке, установить приложение удаленного доступа, подтвердить вход в банковское приложение либо даже лично выполнить перевод. Формально электронная операция в таких случаях подтверждается идентификационными средствами владельца. В то же время фактическое решение о распоряжении денежными средствами основано на ложном представлении: о личности звонящего, назначении платежа, угрозе блокировки счета, необходимости «защитить» деньги или получить несуществующую услугу. Еще сложнее случаи, когда первоначальный обман используется лишь для получения доступа к устройству, после чего перевод выполняется уже без участия потерпевшего. В такой конструкции момент окончания обмана, момент утраты контроля над платежным средством и момент непосредственного изъятия денежных средств не всегда совпадают.

Эта проблема усиливается особенностями платежного законодательства. Закон Республики Узбекистан от 1 ноября 2019 года № ЗРУ-578 «О платежах и платежных системах» определяет платежный инструмент как платежный документ или средство электронного платежа, на основании либо с использованием которого осуществляется платеж. В соответствии со статьей 34 Закона средствами электронного платежа являются банковская карта или иной электронный носитель, содержащий информацию и позволяющий плательщику осуществлять платеж. При этом платежи с использованием средств электронного платежа осуществляются на основании согласия держателя, подтвержденного посредством идентификационных средств. Статья 35 допускает существование банковской карты в виртуальной форме, без физического носителя, а статья 37 отдельно регулирует последствия несанкционированного использования банковской карты. Таким образом, отраслевое законодательство связывает действительность платежной операции с электронным подтверждением согласия, тогда как уголовно-правовая квалификация требует оценки реального содержания воли потерпевшего. Именно несовпадение технического подтверждения операции и фактического волеизъявления образует одну из центральных проблем цифрового мошенничества.

Масштаб проблемы подтверждается официальными данными Министерства внутренних дел Республики Узбекистан. По опубликованным МВД сведениям, в 2019 году с использованием информационных технологий было совершено 863 преступления 18 видов, тогда как в 2024 году зарегистрировано уже 58 800 преступлений 62 видов. Доля киберпреступлений в общей преступности выросла с 6,2 процента в 2023 году до 44,4 процента в 2024 году. При этом 98 процентов киберпреступлений были связаны с банковскими картами и квалифицировались преимущественно как киберкражи и кибермошенничество. Около 60 процентов таких преступлений совершались путем получения контроля над банковской картой или мобильным устройством через вредоносные ссылки и программы, еще 16 процентов – путем получения SMS-кода, подтверждающего управление банковской картой и аккаунтами в мобильных приложениях. Общая сумма похищенных денежных средств, указанная МВД, превысила 1 трлн 909 млрд сумов. Эти показатели свидетельствуют, что вопрос разграничения способов цифрового хищения имеет не единичный, а массовый характер.

Зарубежное регулирование показывает различные подходы к описанию аналогичных деяний. В Европейском союзе Директива (ЕС) 2019/713 от 17 апреля 2019 года о борьбе с мошенничеством и подделкой безналичных средств платежа использует более детализированную систему составов. Статья 2 включает в понятие безналичного платежного инструмента как материальные, так и нематериальные защищенные устройства, объекты или записи, позволяющие переводить деньги или денежную стоимость, в том числе посредством цифровых средств обмена. Статьи 3–5 отдельно охватывают мошенническое использование похищенных, незаконно полученных, поддельных или нематериальных платежных инструментов. Статья 6 выделяет мошенничество, связанное с информационными системами, когда перевод денег, денежной стоимости или виртуальной валюты вызывается незаконным вмешательством в работу системы либо введением, изменением, удалением или передачей компьютерных данных. Такая конструкция демонстрирует разграничение по непосредственному механизму цифрового воздействия, а не только по общему признаку использования информационных технологий.

В Великобритании Fraud Act 2006 построен иначе и сохраняет технологически нейтральную модель. Раздел 2 устанавливает ответственность за мошенничество путем ложного представления, если лицо нечестно сообщает ложные или вводящие в заблуждение сведения с намерением получить выгоду либо причинить другому лицу убыток или риск убытка. Для квалификации не имеет принципиального значения, передается ли ложная информация лично, через телефон, электронную почту, сайт или цифровую платформу. Одновременно раздел 7 предусматривает отдельную ответственность за изготовление, адаптацию, поставку или предложение средств, предназначенных для использования при совершении мошенничества. В результате уголовно-правовая оценка концентрируется на содержании обмана и назначении используемого цифрового средства, а технология выступает прежде всего формой реализации преступного намерения.

Высокая распространенность цифрового финансового обмана характерна и для США. По данным Федеральной торговой комиссии США, в 2025 году потребители

направили около 3 млн сообщений о мошенничестве и указали совокупные потери в размере 15,9 млрд долларов, тогда как в 2024 году сообщалось о потерях свыше 12 млрд долларов. Более 1 млн обращений в 2025 году относились к мошенничеству с выдачей себя за другое лицо, а потери по инвестиционным мошенническим схемам достигли 7,9 млрд долларов. Эти данные важны не только как показатель масштаба: значительная часть современных схем основана не на техническом взломе как таковом, а на получении от самого потерпевшего реквизитов, кодов доступа, подтверждений или перевода денежных средств под воздействием ложной информации.

Таким образом, цифровые платежные инструменты создают для уголовно-правовой квалификации двойственную ситуацию. С одной стороны, электронное подтверждение операции способно фиксировать внешнее волеизъявление владельца. С другой стороны, такое подтверждение может быть получено путем обмана, выполнено под полным контролем злоумышленника либо вообще использоваться только как промежуточный этап для последующего несанкционированного списания. Поэтому граница между мошенничеством с использованием информационных технологий и иными формами хищения проходит не по факту применения банковского приложения, карты, телефона или SMS-кода, а по фактическому механизму завладения денежными средствами и роли в нем воли потерпевшего. Рост количества преступлений, связанных с банковскими картами, делает эту квалификационную проблему одной из наиболее практически значимых для современной уголовно-правовой оценки экономических преступлений в условиях цифровизации.

Adabiyotlar, References, Литературы:

1. Уголовный кодекс Республики Узбекистан от 22 сентября 1994 года № 2012-XII, ст. 168 (в действующей редакции с учетом Закона Республики Узбекистан от 22 июня 2026 года № ЗРУ-1155). Национальная база данных законодательства LexUZ.
2. Постановление Пленума Верховного суда Республики Узбекистан от 23 июня 2023 года № 17 «О судебной практике по делам о мошенничестве», пп. 22, 26. LexUZ.
3. Закон Республики Узбекистан от 1 ноября 2019 года № ЗРУ-578 «О платежах и платежных системах», ст. 34–37, 39–43. LexUZ.
4. Министерство внутренних дел Республики Узбекистан. Материалы по состоянию киберпреступности: сведения, опубликованные 29 мая 2025 года (58 800 преступлений в 2024 году; 98% – преступления, связанные с банковскими картами). Официальный портал gov.uz.
5. Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment, Articles 2–7. EUR-Lex.
6. Fraud Act 2006 (United Kingdom), sections 2 and 7. UK Public General Acts 2006 c.35.
7. U.S. Federal Trade Commission. Testimony before the Joint Economic Committee on the rising scam economy, 25 March 2026: consumer fraud reports and losses for 2025.