

ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С БИТКОЙНАМИ, КРИПТОВАЛЮТАМИ И ДРУГИМИ НОВЕЙШИМИ ЭЛЕКТРОННЫМИ СРЕДСТВАМИ ПЛАТЕЖА

Султонов Нодирбек Улугбекович

<https://doi.org/10.5281/zenodo.17477830>

Аннотация. В статье проводится комплексный анализ преступлений, совершаемых с использованием биткойнов, криптовалют и иных современных электронных средств платежа. Рассматриваются особенности их правовой природы, специфика функционирования в условиях децентрализации и технологической анонимности, а также проблемы правового регулирования, квалификации и расследования данных деяний. Особое внимание уделено сравнительному анализу уголовно-правовых подходов в различных юрисдикциях — Европейском Союзе, США, Российской Федерации и Республике Узбекистан.

Сформулированы предложения по совершенствованию уголовного законодательства и усилению международного сотрудничества в сфере противодействия цифровым преступлениям. Делается вывод о необходимости выработки единой международной терминологии, внедрения специальных уголовно-правовых составов и развития цифровой криминалистики для эффективной борьбы с преступлениями, совершаемыми посредством виртуальных активов.

Ключевые слова: биткойн; криптовалюта; электронные средства платежа; киберпреступления; уголовное право; ФАТФ; Будапештская конвенция; легализация доходов; цифровые активы; Республика Узбекистан; правовое регулирование; кибермошенничество; финансовая безопасность; международное сотрудничество.

GENERAL CHARACTERISTICS OF CRIMES RELATED TO BITCOIN, CRYPTOCURRENCIES, AND OTHER LATEST ELECTRONIC PAYMENT MEANS

Abstract. This article provides a comprehensive analysis of crimes committed using Bitcoin, cryptocurrencies, and other modern electronic payment methods. It examines their legal nature, the specifics of their operation in the context of decentralization and technological anonymity, as well as the issues of legal regulation, classification, and investigation of these crimes. Particular attention is paid to a comparative analysis of criminal law approaches in various jurisdictions—the European Union, the United States, the Russian Federation, and the Republic of Uzbekistan.

Proposals for improving criminal legislation and strengthening international cooperation in combating digital crimes are formulated. The article concludes that it is necessary to develop a unified international terminology, implement specialized criminal law provisions, and develop digital forensics to effectively combat crimes committed through virtual assets.

Keywords: Bitcoin; cryptocurrency; electronic payment systems; cybercrime; criminal law; FATF; Budapest Convention; money laundering; digital assets; Republic of Uzbekistan; legal regulation; cyberfraud; financial security; international cooperation.

Введение

Эволюция цифрового пространства кардинально трансформировала область финансов, дав жизнь инновационным методам платежей, в основе которых лежат электронные средства и цифровые валюты. В то время как классические системы

платежей находились под эгидой государственных структур и банков, появление независимых (децентрализованных) механизмов — в первую очередь, биткойна и смежных криптовалют — сформировало принципиально новую среду, где денежные операции могут реализовываться в обход банковской инфраструктуры. Результатом стало не только расширение горизонта экономических перспектив, но и появление свежих типов криминальных деяний, что требует пересмотра норм уголовного права и актуализации процессов правоприменения.

Тема уголовно-правового анализа действий, реализуемых с применением цифровых валют и других электронных платежных инструментов, приобрела особую значимость на фоне увеличения числа инцидентов, ассоциированных с легализацией незаконных доходов, мошенничеством в киберпространстве, шантажом и финансированием террористической деятельности.

Правовая природа криптовалют и новейших электронных платежных средств

Криптоактив является цифровым имуществом, функционирующим на базе технологии децентрализованной базы данных (блокчейна). В отличие от электронных денежных средств, подлежащих государственному регулированию, цифровые валюты не имеют единственного эмитента и функционируют в условиях децентрализованной инфраструктуры. Их основные характеристики — анонимность и отсутствие централизованного надзора — создают сложности при их юридической классификации.

Глобальные структуры, особенно, **Финансовая группа по разработке мер борьбы с отмыванием денег (ФАТФ)**, считают целесообразным классифицировать цифровые валюты как «виртуальные активы», которые должны подлежать нормативному надзору в контексте действий, направленных на противодействие легализации доходов, полученных преступным путем, и финансированию террористической деятельности. В обновленных руководящих принципах ФАТФ (2019 год) определяется термин «поставщик услуг в сфере виртуальных активов» (VASP), что указывает на императив идентификации сторон, участвующих в операциях, и необходимость контроля за обращением этих цифровых средств.

Важно отметить, что в правовом поле Европейского Союза криптовалюты также не признаны легитимным платежным инструментом; они рассматриваются скорее, как средство обмена или объект для инвестиций. Согласно Директиве ЕС 2018/843 (Пятая директива по борьбе с отмыванием денег, AML), впервые был установлен законодательный императив для криптобирж регистрироваться, подпадать под контроль и проводить обязательную верификацию своих клиентов во время осуществления транзакций.

В Соединенных Штатах Америки контроль за работой с виртуальными валютами возложен на Комиссию по ценным бумагам и биржам (SEC) и Службу по борьбе с финансовыми преступлениями (FinCEN). Эти органы присваивают некоторым цифровым активам статус ценных бумаг или объектов, приравненных к денежным средствам.

Что касается **Российской Федерации**, то юридическое положение криптовалют зафиксировано в Федеральном законе № 259-ФЗ "О цифровых финансовых активах" (от 2020 года). При этом использование таких активов для расчётов на территории страны находится под запретом. В Республике Узбекистан схожие запреты были введены Указом Президента № ПП-3832 (от 2018 года). При этом деятельность площадок для обмена криптовалют (криптобирж) допускается, но только при наличии соответствующей

лицензии.

Классификация преступлений, связанных с криптовалютами и электронными средствами платежа

Деяния уголовного характера, связанные с применением "электронной валюты" (криптовалют) и других цифровых механизмов, охватывают следующие аспекты:

1. Хищение и неправомерное завладение цифровыми фондами — добыча криптовалютных запасов путем обманных действий или злоупотребления уровнем доверия (например, организация подставных предложений токенов (ICO), атаки с целью выманивания учетных данных (фишинг)).

2. Легализация (отмывание) капиталов, добытых преступным путем — трансформация нелегально приобретенных финансов в криптоактивы с последующей их обратной заменой на бумажные деньги для маскировки источника их происхождения.

3. Вымогательство и шантаж — выдвижение требования выплаты откупа в криптовалюте за возвращение конфиденциальной информации или остановку сетевой агрессии (наиболее известный образец — программы-вымогатели).

4. Несанкционированный товарооборот и оборот запрещенной продукции — использование криптосредств для расчетов за наркотические вещества, оружие, поддельные удостоверяющие документы в сегменте "теневого интернета" (даркнет).

5. Финансирование терроризма — передача денежных средств в форме криптовалюты в интересах радикальных групп, обходя стандартные банковские процедуры контроля.

6. Посягательство на целостность правил управления и обращения цифровых сбережений — несанкционированное проникновение в электронные хранилища (кошельки), внедрение вредоносного программного обеспечения для кражи личных данных и токенов.

Подобные правонарушения выделяются повышенной степенью скрытности, трудностями в процессе сбора доказательств и транснациональным охватом, что неизбежно требует привлечения специализированных подразделений кибербезопасности и применения экспертных методик в области цифровой криминалистики.

Проблемы квалификации и расследования криптовалютных преступлений

Ключевая трудность при юридической оценке состоит в том, что в законодательстве отсутствует прямое регулирование, вводящее уголовное преследование за неправомерные действия, связанные с цифровыми валютами. В большинстве государств правовая квалификация в уголовном поле происходит путем сопоставления с уже известными преступными деяниями: либо направленными против частной собственности, либо затрагивающими сферу экономики.

К примеру, неправомерное завладение криптовалютными активами может быть определено как тайное хищение, то есть кражей (по статье 169 Уголовного кодекса Республики Узбекистан), если есть возможность доказать факт причинения материального ущерба. В то же время часто возникает дилемма: допустимо ли рассматривать цифровую валюту как «собственность» в соответствии с правовыми нормами? Отдельные судебные инстанции в Евросоюзе и Соединенных Штатах уже официально признали такие активы предметом имущественных отношений, что существенно облегчает их охрану инструментами уголовного права.

Выявление и расследование подобных правонарушений затруднено ввиду

обезличенного характера операций и отсутствия единой управляющей (центральной) базы для хранения информации. С целью установления личностей, участвующих в преступлениях, применяются специализированные методы исследования сети блокчейн (blockchain forensics), а также активизируется международное взаимодействие через структуры, такие как Европол, Интерпол и Группа «Эгмонт».

Международно-правовые и сравнительно-правовые аспекты

На глобальном уровне наблюдается фокусирование усилий международных структур на формировании унифицированных механизмов контроля за обращением цифровых валют. Такие организации, как ФАТФ, Международный Валютный Фонд и Всемирный банк, акцентируют внимание на критической важности достижения полной прослеживаемости финансовых операций и однозначной верификации владельцев активов.

Важнейшим инструментом в структуре Совета Европы является Конвенция о преступности в сфере компьютерной информации (также известная как Будапештская конвенция, принятая в 2001 году). Этот документ служит основополагающей платформой для противодействия противоправным деяниям, совершаемым в цифровом пространстве. Несмотря на отсутствие прямого упоминания криптовалют, стандарты Конвенции эффективно применяются при расследовании несанкционированного проникновения в системы, кибервзломов и мошеннических действий с использованием компьютерных технологий.

Соединённые Штаты Америки оперируют широким спектром законодательных норм, включая такие ключевые акты, как Computer Fraud and Abuse Act и Bank Secrecy Act. Эти инструменты позволяют осуществлять уголовное преследование индивидов, применяющих цифровые активы для совершения противозаконных действий.

В Российской Федерации и Республике Узбекистан прослеживается курс на планомерное интегрирование цифровых активов в существующие правовые рамки. Тем не менее, нормативно-правовое регулирование в сфере уголовного права в этом сегменте пока характеризуется недостаточной систематизацией. Экспертное сообщество и представители законодательных органов сходятся во мнении о насущной потребности в формулировании специализированных уголовных составов, направленных на борьбу с незаконными операциями, связанными с криптовалютами.

Заключение

Следовательно, неправомерные действия, осуществляемые посредством биткоина, других видов криптовалют и прочих электронных платежных средств, формируют собой совершенно иной класс рисков, выходящих за границы традиционных видов экономических правонарушений. Их определяющими чертами выступают одновременно высокий уровень технологической сложности, гарантирование анонимности и отсутствие привязки к конкретным географическим юрисдикциям.

Действующее уголовное право в большинстве стран лишь фрагментарно отвечает этим современным вызовам. Для успешной борьбы с ними необходимо принять ряд мер, таких как:

- 1) установление единой международной терминологии и определений;
- 2) совершенствование механизмов взаимодействия между странами в процессе проведения расследований;
- 3) введение специальной уголовно-правовой ответственности за совершение

операций с виртуальными активами вне правового поля;

4) методичное повышение квалификации и уровня цифровой осведомленности сотрудников правоприменительных структур.

Модернизация уголовно-правовой базы, учитывающая специфику обращения криптовалютных средств, является неотъемлемым условием для поддержания системы экономической безопасности и обеспечения законности в условиях стремительного перехода к цифровой экономике.

REFERENCES

1. Указ Президента Республики Узбекистан № ПП–3832 от 3 июля 2018 г. «О мерах по организации деятельности по обращению криптоактивов».
2. Постановление Президента Республики Узбекистан № ПП–6819 от 14 декабря 2021 г. «О мерах по дальнейшему развитию цифровых технологий».
3. Закон Республики Узбекистан «Об электронных платежах» от 2 сентября 2019 г. № ЗРУ–573.
4. Федеральный закон Российской Федерации от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».
5. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Fifth Anti-Money Laundering Directive).
6. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets (MiCA).
7. FATF (Financial Action Task Force). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris: FATF/OECD, 2021.
8. Council of Europe. *Convention on Cybercrime* (Budapest Convention), 2001.
9. United States Congress. *Computer Fraud and Abuse Act (CFAA)*, 1986.
10. United States Congress. *Bank Secrecy Act (BSA)*, 1970.
11. United States v. Larry Dean Harmon, Case No. 1:19-cr-00395 (D.D.C., 2021).
12. International Monetary Fund. *Virtual Currencies and Beyond: Initial Considerations*. Washington, D.C., 2016.
13. World Bank. *Regulating Virtual Currencies: The Case of Bitcoin and Beyond*. Policy Research Working Paper, 2019.