УДК 34

РАСКРЫТИЕ ВЗЯТОЧНИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

UNCOVERING BRIBERY COMMITTED USING INFORMATION AND TELECOMMUNICATIONS TECHNOLOGIES

Динар Минзеферович Фарахиев,

независимый исследователь

dfarakhiev@mail.ru

Ключевые слова:
коррупция,
взяточничество,
ИТТ,
цифровое взяточничество,
криптовалюты,
оперативно-розыскная деятельность,
доказывание,
электронные доказательства.

В статье проводится комплексный анализ современных тенденций и специфики совершения преступлений, связанных со взяточничеством, с активным использованием информационно-телекоммуникационных технологий (далее – ИТТ). Рассматриваются новые формы взяточничества, такие как «электронные взятки», использование криптовалют и зашифрованных каналов связи для переговоров о даче и (или) получении предмета незаконного вознаграждения. Особое внимание уделено проблемам доказывания в условиях цифровизации общественных отношений, а также разработке эффективных криминалистических и оперативно-розыскных методик, направленных на выявление и фиксацию исследуемых видов преступлений. Предлагаются меры по совершенствованию законодательной базы и правоприменительной практики для противодействия взяточничеству в цифровой среде.

Keywords:
corruption,
bribery,
information technology,
digital bribery,
cryptocurrencies,
operational-investigative activities,
proof,
electronic evidence.

This article provides a comprehensive analysis of current trends and specifics of bribery-related crimes committed with the active use of information and telecommunications technologies (further – ITT). New forms of bribery, such as «electronic bribes», the use of cryptocurrency, and encrypted communication channels for negotiations regarding the payment and/or receipt of illegal remuneration, are examined. Particular attention is paid to the problems of proof in the context of the digitalization of social relations, as well as the development of effective forensic and

investigative methods aimed at identifying and recording these types of crimes. Measures are proposed to improve the legislative framework and law enforcement practices to combat bribery in the digital environment.

Прогрессирующее проникновение ИТТ во все сферы общественной жизни неизбежно трансформирует и криминальную среду. Взяточничество, являясь одним из наиболее общественно опасных коррупционных преступлений, адаптируется к новым технологическим реалиям, приобретая новые, зачастую менее очевидные формы. Традиционные методы выявления и документирования преступлений, основанные на физическом контакте и передаче материальных ценностей, становятся недостаточными для эффективного противодействия «цифровому взяточничеству».

Актуальность данного исследования обусловлена прежде всего необходимостью пересмотра существующих криминалистических подходов и тактик ОРД с учетом специфики использования современных технологий, средств связи, шифрования и цифровых платежных систем. В данном контексте нельзя не согласиться с мнение профессора П.И. Иванова, который утверждает, что «современные тенденции, как правило, определяются наличием множества факторов, и прежде всего носящих социально-экономический (экономический кризис, существование криптовалюты, внутренний аудит, банкротство, использование фирм-однодневок, теневой финансовый поток) правовой (модернизация закупочной деятельности) и организационный характер (идентификация цифровой личности)» [2, с. 321].

Классическое понимание предмета взятки – деньги, материальные ценности – существенно расширилось. В контексте использования ИТТ взятка может принимать форму безналичных перечислений через сложные многоступенчатые схемы, использование криптовалют [3; 5] (например, Monero, Zcash), предоставление доступа к закрытым информационным ресурсам или даже «вознаграждение» в виде прав на интеллектуальную собственность, полученное через цифровые платформы. На наш взгляд, развитие новых форм предмета взяточничества усложняет установление причинно-следственной связи между получением выгоды и совершением «должностного действия», а также затрудняет процедуру ареста и конфискации предмета преступления, что мы не раз аргументировали в своих работах[1].

1 См., напр.: Фарахиев Д.М. Взяточничество в условиях цифровизации: новые вызовы, проблемы и пути решения // Искусство правоведения. 2025. № 3(15). С. 155-164; Фарахиев Д.М. Конфискация имущества, приобретенного в результате совершения преступления, предусмотренного ст. 290 УК РФ // Мониторинг правоприменения. 2023. № 1(46). С. 37-43.

Особую опасность представляет использование мессенджеров с функцией сквозного шифрования, таких как Telegram или WhatsApp[1], для обсуждения условий «сделки». По мнению автора статьи, использование данных мессенджеров создает «невидимый» канал коммуникации между преступниками, где информация, являющаяся прямым доказательством сговора, недоступна для стандартных методов негласного получения информации, требуя применения более сложных методов криптоанализа или получения данных через международное сотрудничество.

Раскрытие взяточничества, опосредованного ИТТ, требует глубокой интеграции традиционной криминалистики с «цифровой криминалистикой» [подр.: 7, с. 233]. Центральной проблемой становится легитимная фиксация электронных доказательств, а равно использование цифровых следов в качестве доказательной базы при документировании преступной деятельности [1, с. 24]. К ним относятся логи серверов, метаданные файлов, история переписки, данные геолокации устройств, а также информация из облачных хранилищ.

Вместе с тем нельзя не отметить, что процедура изъятия и осмотра электронных носителей информации должна строго соответствовать процессуальным нормам, чтобы обеспечить допустимость полученных данных в процессе предварительного расследования, а в дальнейшем – в суде. Несоблюдение правил сохранения целостности цифрового следа (например, нарушение цепочки хранения) может привести к признанию ключевых доказательств недействительными и (или) недопустимыми [6, с. 120-128]. В связи с этим необходима постоянная подготовка специалистов, владеющих методиками создания криминалистически значимых образов дисков и анализа цифровых транзакций, способных доказать факт передачи, получения или предложения взятки.

Традиционные оперативные комбинации, связанные с «контролируемой передачей предмета взятки», трансформируются в «контролируемое перечисление» или «контролируемое предоставление доступа», что, на наш взгляд, требует от сотрудников подразделений экономической безопасности и противодействия коррупции, правомочных в полном объеме осуществлять ОРД[2], глубокого понимания принципов работы блокчейна, анонимных сетей (Tor) и методов обфускации данных. В данной связи большое внимание уделяется именно системе блокчейн, которая рассматривается авторами как «эффективный способ борьбы с коррупцией» и «может быть применим в России, однако для ее успешной реализации необходимо учитывать особенности функционирования правовой системы нашего государства, тенденции распространения

1 Принадлежит американской корпорации Meta (признана в России экстремистской и запрещена). Мессенджер внесен Роскомнадзором в реестр организаторов распространения информации.

2 Об утверждении Перечня оперативных подразделений органов внутренних дел Российской Федерации, правомочных осуществлять оперативно-розыскную деятельность : приказ МВД России от 31.03.2023 № 199. Здесь и далее, если не оговорено иное, нормативные правовые акты находятся в СПС «КонсультантПлюс».

коррупции в определенных сферах экономики и государственного управления, а самое главное, наличие современных информационных технологий» [4, с. 41].

Вместе с тем при выявлении фактов использования криптовалют в качестве предмета незаконного вознаграждения, стандартные процедуры отслеживания финансовых потоков оказываются неэффективными. В таких случаях тактика ОРД должна быть направлена на установление «точек входа» и «точек выхода» средств, то есть моментов конвертации криптовалюты в фиатные деньги или приобретения на них материальных благ, а также на выявление IP-адресов и устройств, с которых осуществлялись транзакции, используя методы «сетевой криминалистики». Важным инструментом становится анализ цифрового следа, оставленного лицом, совершающим преступление, даже при использовании средств анонимизации.

Принимая во внимание специфику противоправной деятельности, мы выявили возможную схему совершения преступных транзакций, связанных со взяточничеством:

– денежные средства переводятся с электронного кошелька или лицевого счета взяткодателя (посредника) на платежные реквизиты обменника (биржи);

– в обменнике (на бирже) происходит конвертация российских рублей в криптоактивы;

– с криптокошелька обменника (биржи) криптоактивы поступают на криптокошелек взяткополучателя (посредника);

– взяткополучатель (посредник) осуществляет перевод криптоактивов с криптокошелька на криптовалютный соответствующий кошелек обменника (биржи);

– в обменнике (на бирже) происходит конвертация криптоактивов в фиатные денежные средства (российские рубли, доллары США и прочее);

– с обменника (биржи) на лицевой счет взяткополучателя (посредника) (либо электронный кошелек) зачисляются конвертированные денежные средства.

После конвертации криптоактивов в фиатные денежные средства они включаются в законный гражданско-правовой оборот, им придается правомерный вид владения, а также пользования и распоряжения ими[1].

Основной вызов в делах о «цифровом взяточничестве» – это доказывание субъективной стороны преступления (умысла) и установление факта получения выгоды, когда она не является очевидной (например, предоставление доступа к инсайдерской информации или услуге). В отличие от наличных денежных средств, цифровая выгода часто замаскирована под легитимные транзакции или вознаграждения за консультационные услуги и пр.

1 Подробнее данная схема нами раскрыта в: Фарахиев Д.М. Оперативно-розыскная деятельность органов внутренних дел в противодействии взяточничеству, совершаемому с использованием цифровых финансовых и криптовалютных активов // Вестник Казанского юридического института МВД России. 2025. Т. 16. № 1(59). С. 127-137.

Для преодоления этой сложности криминалистика может предложить усиление роли заключения экспертов. Результаты компьютерно-технических экспертиз должны не только подтверждать подлинность сообщений или файлов, но и интерпретировать их содержание в контексте оперативной информации, доказывая коррупционную подоплеку. Важно также уделять внимание анализу поведения должностного лица до и после предполагаемого получения выгоды, используя методы поведенческого анализа, сопоставляя его действия с известными цифровыми следами.

Также нельзя не сказать о том, что действующее законодательство, регулирующее доказательственную базу и ОРД, часто запаздывает по отношению к развитию технологий, поскольку в настоящее время существует потребность в уточнении правового статуса электронных сообщений, полученных из закрытых источников, а также в унификации процедур международного сотрудничества для получения данных от зарубежных интернет-провайдеров и операторов связи.

Принимая во внимание вопрос межведомственного и международного сотрудничества, следует отметить, что Федеральным законом от 1 апреля 2025 г. № 41-ФЗ в Федеральный закон «Об оперативно-розыскной деятельности» внесены изменения, касающиеся проведения оперативно-розыскного мероприятия «наведение справок». Согласно изменениям: при наличии технической возможности и с соблюдением мер по обеспечению конфиденциальности и безопасности передаваемой информации в целях наведение справок может использоваться единая система межведомственного электронного взаимодействия. На наш взгляд, это нововведение позволит значительно повысить эффективность ОРД путем ускорения процессов обмена оперативно-розыскной информацией между различными ведомствами и государственными структурами в процессе выявления, документирования и раскрытия исследуемых видов преступлений. Использование единой системы межведомственного электронного взаимодействия обеспечит оперативность получения необходимых сведений, минимизирует временные затраты и снизит вероятность ошибок при передаче данных.

Отметим, что ранее нами предлагались иные формулировки для внесения соответствующих изменений (ст. 8 и ст. 15 Федерального закона «Об оперативно-розыскной деятельности»), которые, по мнению автора статьи, нормализуют порядок и сроки предоставления сведений и повысят эффективность выявления и документирования взяточничества, совершаемого (совершенного) с использованием ИТТ[1].

На организационном уровне необходимо поставить вопрос о создании специализированных подразделений, обладающих компетенциями в области финансового анализа криптотранзакций и глубокого технического анализа

1 См.: Фарахиев Д.М. Наведение справок как инструмент сбора компрометирующих сведений в отношении должностных лиц, причастных к совершению взяточничества // Вестник Сибирского юридического института МВД России. 2025. № 3(60). С. 243-249.

полученных данных. Регулярное повышение квалификации сотрудников органов внутренних дел Российской Федерации в сфере ИТТ, а также развитие междисциплинарного взаимодействия между юристами, IT-специалистами и криминалистами, являются ключевыми условиями для повышения эффективности раскрытия «цифрового взяточничества». Так, большой интерес вызывает анализ платформы по безопасности цифровых активов «Шард». Инструментарий данной платформы дает возможность пользователям провести «расследование» и получить аналитическую и правовую помощь. Платформа «Шард» по безопасности цифровых активов оказывает пользователям следующие услуги: проверка криптоадресов, граф транзакций, разработка блокчейн-решений, блокчейн-аналитика и исследования и пр.

Таким образом, можно констатировать, что взяточничество, совершающееся (совершенное) с использованием ИТТ, представляет собой сложную, динамично развивающуюся угрозу национальной, экономической и общественной безопасности. Успешное противодействие этому явлению требует не просто адаптации существующих методик, но и их коренной перестройки. Фокус должен сместиться с материального носителя на информационное содержание и цифровой след. Только комплексный подход, сочетающий передовые криминалистические методы фиксации электронных доказательств, инновационные тактики ОРД и своевременное совершенствование законодательной базы, позволит обеспечить адекватное правовое реагирование на вызовы цифровой коррупции. Дальнейшие исследования должны быть направлены на разработку процессуально закрепленных стандартов работы с анонимными цифровыми активами как предметом преступления.

Библиографический список

1. Выявление и раскрытие преступлений подразделениями экономической безопасности и противодействия коррупции органов внутренних дел по отдельным направлениям деятельности : учебное пособие / Р.Г. Искалиев, М.И. Мамаев, А.В. Телков [и др.]. – М.: Академия управления МВД России, 2024. – 216 с.

2. Иванов, П.И. Современное состояние и перспективы развития экономической и коррупционной преступности (авторское обоснование) / П.И. Иванов // Аграрное и земельное право. – 2025. – № 3. – С. 320-325.

3. Корольков, Д.А. Криптовалюта как предмет взятки / Д.А. Корольков // Молодые исследователи и наука: актуальные вопросы, достижения и инновации : сборник статей по материалам III всероссийской (с международным участием) студенческой научно-практической конференции, Йошкар-Ола, 23–24 ноября 2023 года. – Йошкар-Ола: АНО ВО «Межрегиональный открытый социальный институт», 2023. – С. 157-163.

4. Куликов, А.В. Современный способ борьбы с коррупцией – использование технологии блокчейн / А.В. Куликов, Д.А. Символокова // Известия Тульского государственного университета. Экономические и юридические науки. – 2021. – № 4. – С. 36-42.

5. Никонов, П.В. Цифровые финансовые активы и цифровая валюта, как предмет взяточничества / П.В. Никонов // Искусство правоведения. – 2023. – № 1(5). – С. 71-74.

6. Особенности и проблематика использования результатов оперативно-розыскной деятельности в качестве доказательств в уголовном процессе / Е.Ю. Андреева, Е.В. Быкадорова, П.Д. Смешнов, В.Н. Лебедев // Северо-Кавказский юридический вестник. – 2021. – № 1. – С. 120-128.

7. Фарахиев, Д.М. Некоторые особенности криминалистической характеристики способов совершения взяточничества в условиях цифровизации общественных отношений / Д.М. Фарахиев // Вестник Российской правовой академии. – 2025. – № 3. – С. 227-236.