



Научная статья

УДК 34

<https://doi.org/10.33874/2072-9936-2025-0-3-227-236>

НЕКОТОРЫЕ ОСОБЕННОСТИ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ СПОСОБОВ СОВЕРШЕНИЯ ВЗЯТОЧНИЧЕСТВА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВЕННЫХ ОТНОШЕНИЙ

Динар Минзеферович Фарахиев

Академия управления МВД России, 125993, Россия, г. Москва,
ул. Зои и Александра Космодемьянских, д. 8

dfarakhiev@mail.ru

Аннотация

Актуальность настоящего исследования обусловлена ростом количества регистрируемых фактов взяточничества в цифровом пространстве, а также необходимостью осознания и понимания новых форм их совершения, возникающих в результате внедрения и развития информационно-телекоммуникационных технологий. В условиях анонимности транзакций преступники-взяточники находят все более изощренные способы сокрытия своих противоправных действий от органов внутренних дел РФ, которые ежегодно выявляют более 80% фактов взяточничества. Кроме того, в работе освещаются ключевые проблемы, связанные с методами совершения исследуемых преступлений, что позволяет глубже понять особенности совершения взяточничества в условиях цифровизации общественных отношений. Это способствует выработке методов их выявления и документирования, а также определению мер по минимизации подобных правонарушений. Цель настоящего исследования – выявить отдельные отличительные аспекты криминалистической характеристики способов совершения взяточничества в условиях цифровизации общественных отношений. Методологическая основа включает положения диалектического метода познания, а также методы формально-юридического и логического анализа, индукции и дедукции. Автор приходит к выводу о том, что борьба со взяточничеством в условиях цифровизации требует от органов внутренних дел РФ комплексного подхода, который включает как теоретические, так и практические меры. Такой подход должен опираться на новые способы совершения преступлений и учитывать особенности цифровых технологий для эффективного выявления и пресечения противоправных действий.

Ключевые слова: преступность; взяточничество; цифровизация; способы совершения; криминалистика; оперативно-разыскная деятельность; органы внутренних дел Российской Федерации; цифровые финансовые активы; криптовалютные активы; анонимность.

Для цитирования: *Фарахиев Д. М.* Некоторые особенности криминалистической характеристики способов совершения взяточничества в условиях цифровизации общественных отношений // Вестник Российской правовой академии. 2025. № 3. С. 227–236. <https://doi.org/10.33874/2072-9936-2025-0-3-227-236>

Research Article

SOME FEATURES OF FORENSIC CHARACTERISTICS OF METHODS OF COMMITTING BRIBERY IN THE CONDITIONS OF DIGITALIZATION OF PUBLIC RELATIONS

Dinar M. Farakhiev

Academy of the Ministry of Internal Affairs of Russia,
8 Zoya and Alexander Kosmodemianskikh St., Moscow, 125993, Russia
dfarakhiev@mail.ru

Abstract

The relevance of this study is due to the growing number of registered facts of bribery in the digital space, the need to recognize and understand new forms of their commission, which arise as a result of the introduction and development of information and telecommunication technologies. In the conditions of anonymity of transactions, criminals-bribe-takers find more sophisticated ways to conceal their illegal actions from the internal affairs bodies of the Russian Federation, which annually reveal more than 80% of facts of bribery. In addition, the study highlights several key issues related to the consideration of the methods of committing the types of crimes under study, which will allow for a more detailed consideration of the features of bribery in the context of digitalization of public relations, develop methods for their detection and documentation, and identify measures to minimize them. The purpose of this study is to identify individual distinctive aspects of the forensic characteristics of the methods of committing bribery in the context of digitalization of public relations. The methodological basis includes the provisions of the dialectical method of cognition, as well as methods of formal-legal and logical analysis, induction and deduction. In conclusion, the author formulates the conclusion that the fight against bribery in the context of digitalization of public relations requires a comprehensive approach from the internal affairs bodies of

the Russian Federation, which includes both theoretical and practical aspects based on new methods of committing the types of crimes under study.

Keywords: crime; bribery; digitalization; methods of committing; forensics; operational investigative activities; internal affairs agencies of the Russian Federation; digital financial assets; cryptocurrency assets; anonymity.

For citation: Farakhiev D. M. Some Features of Forensic Characteristics of Methods of Committing Bribery in the Conditions of Digitalization of Public Relations. *Herald of the Russian Law Academy*, 2025, no. 3, pp. 227–236. (In Russ.) <https://doi.org/10.33874/2072-9936-2025-0-3-227-236>

Введение

В условиях стремительной цифровизации общественных отношений, когда информационно-телекоммуникационные технологии внедряются во многие сферы жизнедеятельности общества, проблема взяточничества приобретает новые, более сложные и изощренные формы. Взяточничество традиционно ассоциировалось с получением и передачей предмета незаконного обогащения лично или через посредника, однако в настоящее время наблюдается тенденция использования цифровых платформ и виртуальных финансовых инструментов, что вызывает определенные трудности предупредительной деятельности органов внутренних дел Российской Федерации, требуя адаптации существующих методов борьбы и разработки новых подходов к выявлению и документированию преступлений, предусмотренных ст. 290–291.2 Уголовного кодекса РФ (далее – УК РФ).

Криминалистические и оперативно-разыскные методы борьбы со взяточничеством, совершаемым в условиях цифровизации общественных отношений, занимают центральное место в настоящем исследовании. Автором выявляются инструменты и подходы, которые могут применяться в целях выявления и документирования исследуемых видов преступлений, а также какие трудности возникают в процессе борьбы с исследуемыми видами преступлений. Важным аспектом выступает анализ роли информационно-телекоммуникационных технологий в обеспечении анонимности преступников-взяточников, что делает их действия более скрытными.

1. Актуальность проблемы взяточничества в условиях цифровизации общественных отношений

В условиях стремительной цифровизации общественных отношений традиционные формы преступности, в том числе взяточничества, претерпевают значительные трансформации. Развитие информационно-телекоммуникационных технологий и средств коммуникации широко востребовано как в бизнесе, так и в публичном секторе. Как справедливо отмечает профессор А. И. Овчинников, «цифровизация государственного управления, экономики, образования, здравоохранения и других сфер государственной и общественной жизни стала общемировым

трендом» [1, с. 159], поскольку действительно многие сферы жизнедеятельности общества подвергнуты влиянию цифровизации за счет внедрения информационно-телекоммуникационных технологий.

Следует отметить, что в настоящее время использование цифровых финансовых и криптовалютных активов является новеллой для российского общества. При этом данные активы все чаще используются при совершении взяточничества, становясь все более популярными. В этой связи нельзя не согласиться с мнением С. А. Поповой, которая считает, что «дальнейшее развитие информационно-коммуникационных технологий может привести к появлению новых предметов, которые могут быть использованы при осуществлении расчетов в коррупционных целях» [2, с. 81]. На наш взгляд, использование преступниками-взяточниками исследуемых «инструментов» обеспечивает значительную степень анонимности, что затрудняет деятельность органов внутренних дел Российской Федерации по выявлению и документированию фактов взяточничества; обеспечивает высокую степень конфиденциальности и сложность отслеживания транзакций, что создает дополнительные трудности для правоохранителей.

Ключевое значение в современных способах совершения взяточничества в условиях цифровизации общественных отношений имеют технологии искусственного интеллекта и технологии больших данных [3]. Преступники-взяточники используют алгоритмы для анализа данных и выбора наиболее уязвимых объектов. Например, они могут отслеживать поведение пользователей в сети Интернет, выявлять тех, кто имеет высокую степень доверия к различным онлайн-сервисам, и целенаправленно на них воздействовать. Это расширяет арсенал методов, применяемых для совершения взяточничества, и одновременно усложняет задачу для органов внутренних дел Российской Федерации, которым приходится адаптироваться к новым вызовам.

Кроме того, современные преступники-взяточники активно применяют анонимизаторы и VPN-технологии для сокрытия своих противоправных действий, что вызывает определенные трудности для органов внутренних дел Российской Федерации. Применение исследуемых технологий позволяет преступникам-взяточникам безнаказанно совершать противоправные действия, отвлекая внимание правоохранительных органов, в частности органов внутренних дел Российской Федерации, усложняя процесс выявления и документирования фактов взяточничества.

В процессе анализа материалов правоприменительной практики выявлена особенность в преступных схемах, которые могут включать в себя подделки электронных документов и использование фальшивых идентификационных данных. Данные технологии позволяют преступникам-взяточникам создавать виртуальные личности, избегая личной встречи между взяткодателем и взяткополучателем (или посредником), что не только делает процесс анонимным, но и отпугивает потенциальных свидетелей, если они не принимали участие непосредственно.

Кроме того, нами выделяются наиболее распространенные схемы и механизмы совершения преступлений, предусмотренных ст. 290–291.2 УК РФ, с использованием криптовалютных активов:

1) открытие должностным лицом, его родственником и третьими лицами, находящимися в непосредственной связи с взяточполучателем, электронных кошельков и криптокошельков;

2) перечисление криптовалютных активов на открытый ранее электронный кошелек и криптокошелек и передача взяткодателю идентификатора электронного криптокошелька (цифровой код или же QR-код);

3) обмен криптовалютных активов на фиатную валюту с использованием криптовалютных бирж и вывод денежных средств через банкоматы.

Таким образом, можно утверждать, что органы внутренних дел Российской Федерации сталкиваются с необходимостью применения новых методов выявления и документирования фактов взяточничества, в которых предметом незаконного вознаграждения выступают цифровые финансовые и криптовалютные активы, принимая во внимание вышеуказанные схемы и механизмы противоправной деятельности. Кроме того, традиционные подходы становятся менее эффективными в условиях, когда преступники-взяточники используют информационно-телекоммуникационные технологии для осуществления своей противоправной деятельности.

На наш взгляд, взяточничество в условиях цифровизации общественных отношений представляет собой сложные и многогранные преступления, которые требуют иного подхода к их выявлению и документированию, а также расследованию и оперативно-разыскному сопровождению. Криминалистические и оперативно-разыскные методы должны адаптироваться к трансформирующимся условиям, обеспечивая защиту от вышеуказанных угроз и создавая инструменты для успешного противостояния цифровым формам взяточничества. Применение информационно-телекоммуникационных технологий в сочетании с актуальной уголовно-правовой практикой станет залогом успешной реализации мер борьбы с взяточничеством в период активной цифровизации общественных отношений.

2. Роль информационно-телекоммуникационных технологий в обеспечении анонимности лиц, совершающих взяточничество, в условиях цифровизации общественных отношений

Анонимность преступников-взяточников в условиях цифровизации общественных отношений достигается благодаря целому ряду технологических средств, обеспечивающих негласность пользователей в сети Интернет, денежно-финансовых и иных операций и их непрослеживаемость. Использование информационно-телекоммуникационных технологий при совершении взяточничества обеспечивает преступникам возможность обмениваться информацией и проводить денежно-финансовые и иные операции в анонимном режиме, затрудняя идентификацию субъектов противоправной деятельности.

Итак, *информационное пространство* порождает возможность создания поддельных аккаунтов и фальшивых документов, что позволяет преступникам-взяточникам использовать «дублирующиеся» личности. В процессе проведения данных операций преступники зачастую прибегают к услугам скрытых веб-ресурсов, позволяющих анонимно приобретать инструменты и получать информацию, необходимые для совершения взяточничества.

Социальные сети и мессенджеры остаются важными каналами коммуникации, но их использование требует осторожности. Настройки конфиденциальности и шифрование данных и сообщений позволяют преступникам-взяточникам взаимодействовать на более безопасном уровне, однако органы внутренних дел Российской Федерации год за годом активнее пытаются внедрить индивидуальные методы мониторинга.

Ряд преступников-взяточников формируют собственные сети для обмена опытом и доступа к ресурсам. Они могут использовать инструменты обмена сообщениями с высокой степенью безопасности и шифрования, такие как *Signal* или *Telegram*. Таким образом, создание защищенного информационного пространства позволяет им оставаться вне досягаемости для органов внутренних дел Российской Федерации.

Вместе с тем нельзя не сказать об *облачных технологиях*, которые создают условия для хранения данных и документов без физического их присутствия. Это означает, что важная информация между субъектами противоправных правоотношений может быть размещена на серверах, находящихся в юрисдикциях, где законодательство Российской Федерации регулирует их на низком или удовлетворительном уровне. На наш взгляд, данный подход предоставляет дополнительные возможности для совершения квалифицированных и особо квалифицированных составов преступлений, предусмотренных ст. 290–291.2 УК РФ, и, как следствие, освобождения преступников-взяточников от уголовной ответственности и наказания.

На наш взгляд, более широкий доступ к информации и ресурсам позволяет выявлять и документировать противоправные факты о взяточничестве оперативнее и эффективнее, как по времени, так и по ресурсам. Сравнительно с предыдущими периодами, доступ к специализированным знаниям и технологиям стал более демократизированным, что создает парадокс: преступники-взяточники, обладая такими же технологиями, как и органы внутренних дел Российской Федерации, могут обнаруживать и использовать уязвимости в действующем законодательстве и правоприменении.

По мнению автора, комплексная деятельность органов внутренних дел Российской Федерации по выработке и внедрению новых методов выявления и документирования фактов взяточничества в условиях цифровизации общественных отношений, а равно расследования уголовных дел, требует междисциплинарного подхода. Кроме того, необходимо принимать во внимание, что в условиях цифровизации общественных отношений и стремительного развития и внедрения информационно-телекоммуникационных технологий противодействие взяточничеству должно опираться на комплексное понимание преступных схем, используемых преступниками-взяточниками.

3. Перспективы развития криминалистических и оперативно-разыскных знаний в борьбе со взяточничеством в условиях цифровизации общественных отношений

Цифровизация значительно трансформировала не только способы совершения преступлений, предусмотренных ст. 290–291.2 УК РФ, но и методы их выявления, до-

кументирования, предупреждения и расследования, что делает необходимым переосмысление традиционных подходов как в криминалистике, так и в оперативно-разыскной деятельности. Применение информационно-телекоммуникационных технологий в различных сферах открывает новые возможности для совершения взяточничества, создавая платформы для анонимных транзакций и безналичных расчетов. Преступники-взяточники все чаще используют современные средства связи и информационно-телекоммуникационные технологии, чтобы скрыть свою противоправную деятельность, что требует адаптации и развития новых методов, как ранее нами уже было отмечено.

Одной из ключевых задач органов внутренних дел Российской Федерации является создание комплексного подхода к выявлению и документированию фактов взяточничества, а также оперативному сопровождению расследования уголовных дел, включая взаимосвязь между информационно-телекоммуникационными технологиями и уголовным правом. Разработка специализированных инструментов для анализа цифровых (виртуальных) следов, оставленных после совершения транзакций, а также повышение квалификации сотрудников органов внутренних дел Российской Федерации в исследуемой сфере, становится важной задачей. В свою очередь, под цифровым (виртуальным) следом следует понимать: «зафиксированный компьютерной системой на цифровом материальном носителе результат отражения реального (физического) процесса или действия иной компьютерной системы, связанный с преступлением (имеющий уголовно-релевантное значение), в виде цифрового образа формальной модели этого процесса» [4, с. 13].

Большое значение имеет также внедрение технологии больших данных и искусственного интеллекта в криминалистику и оперативно-разыскную деятельность. Нельзя исключать, что информационно-телекоммуникационных технологий при выявлении фактов взяточничества позволяют обрабатывать и анализировать большие объемы информации на предмет выявления аномалий и подозрительных схем поведения должностных лиц, возможно, причастных к совершению взяточничества.

На наш взгляд, вопрос разработки инструментов для анализа использования цифровых финансовых и криптовалютных активов в качестве предмета взяточничества является в настоящее время наиболее актуальным. Цифровые финансовые и криптовалютные активы позволяют преступникам-взяточникам скрывать свою противоправную деятельность, оставаясь анонимными, в силу своей децентрализованной природы и возможности скрыть источник незаконного обогащения и получателя (отправителя) средств.

Важно отметить, что цифровизация открывает новые возможности не только для совершения взяточничества, но и для борьбы с ней [5, с. 143–171]. Одним из направлений может стать применение технологии блокчейна [6, с. 81–87] для создания прозрачных систем учета и контроля, что значительно усложнит процесс совершения преступлений, предусмотренных ст. 290–291.2 УК РФ. Применение технологии блокчейна на уровне государственных (муниципальных) учреждений, в том числе органов внутренних дел Российской Федерации, способствует минимизации коррупционных рисков и количества регистрируемых преступле-

ний, предусмотренных ст. 290–291.2 УК РФ, а также повышению доверия общества и населения к органам власти и их должностным лицам.

Заключение

В заключение настоящего исследования следует отметить, что проблема взяточничества в условиях цифровизации общественных отношений является одной из наиболее актуальных и сложных задач, стоящих перед современным обществом и органами внутренних дел Российской Федерации. С развитием и внедрением информационно-телекоммуникационных технологий во многие сферы жизнедеятельности общества взяточничество приобретает новые формы, что требует от криминалистов и правозащитников (органов, осуществляющих оперативно-разыскную деятельность) адаптации существующих методов и разработки новых подходов к выявлению и документированию фактов взяточничества и оперативно-разыскному сопровождению уголовных дел, возбужденных по признакам составов преступлений, предусмотренных ст. 290–291.2 УК РФ.

Современные виды, формы и способы совершения взяточничества в условиях цифровизации общественных отношений становятся все более распространенными [7, с. 183]. Виртуальные платформы и анонимные транзакции, осуществляемые посредством цифровых финансовых и криптовалютных активов, создают дополнительные сложности для органов внутренних дел Российской Федерации, поскольку они затрудняют отслеживание финансовых потоков и идентификацию участников преступных схем [8, с. 213–221; 9, с. 81–90], что в свою очередь подчеркивает необходимость глубокого анализа и понимания новых технологий, которые используются преступниками-взяточниками как для совершения, так и для сокрытия противоправной деятельности.

Перспективы развития криминалистики и оперативно-разыскной деятельности в условиях цифровизации общественных отношений открывают новые горизонты для исследования и практического применения в области борьбы со взяточничеством. Вместе с тем важно не только адаптировать существующие методы, но и развивать новые подходы, которые будут учитывать специфику цифровой среды в исследуемой проблеме.

Таким образом, в заключение необходимо отметить, что борьба со взяточничеством в условиях цифровизации общественных отношений требует от органов внутренних дел Российской Федерации комплексного подхода, который включает в себя как теоретические, так и практические аспекты. Необходимость постоянного обновления теоретических и практических знаний и навыков, а также адаптации методов выявления и документирования фактов взяточничества к новым условиям является ключевым фактором в успешной борьбе с исследуемыми видами преступлений.

Пристатейный библиографический список

1. Овчинников А. И. Противодействие коррупции в условиях цифровизации: возможности, перспективы, риски // Журнал российского права. 2019. № 11.

2. Попова С. А. Применение цифровых технологий в борьбе с коррупцией // Российский правовой журнал. 2021. № 3 (8).
3. Марц Н., Уоррен Д. Большие данные. Принципы и практика построения масштабируемых систем обработки данных в реальном времени. М. : Вильямс, 2016.
4. Агibalов В. Ю. Виртуальные следы в криминалистике и уголовном процессе : автореф. дис. ... канд. юрид. наук. Воронеж, 2010.
5. Цирин А. М., Черепанова Е. В., Тулинова О. А. Современные стандарты и технологии противодействия коррупции // Журнал российского права. 2014. № 7.
6. Гумаров И. А., Фарахiev Д. М. Технология blockchain как средство противодействия коррупции // Научный компонент. 2022. № 1 (13).
7. Фарахiev Д. М., Минзянова Д. Ф. Трансформация предмета и способа совершения преступлений, предусмотренных ст.ст. 290 и 291 УК РФ в процессе глобализации // Новеллы права, экономики и управления 2022 : материалы VIII Международ. науч.-практич. конф., Гатчина, 25 ноября 2022 года. Т. 1. Гатчина, 2023.
8. Фарахiev Д. М. Деятельность подразделений экономической безопасности и противодействия коррупции по документированию преступлений, совершаемых с использованием цифровых финансовых и криптовалютных активов // Труды Академии управления МВД России. 2023. № 3 (67).
9. Фарахiev Д. М. Деятельность органов внутренних дел в процессе раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий (на примере криптовалютных активов) // Юридический вестник Самарского университета. 2023. Т. 9. № 3.

References

1. Ovchinnikov A. I. Combating Corruption in the Context of Digitalization: Opportunities, Prospects, Risks. *Journal of Russian Law*, 2019, no. 11. (In Russ.)
2. Popova S. A. Application of Digital Technologies in the Fight Against Corruption. *Russian Legal Journal*, 2021, no. 3 (8). (In Russ.)
3. Martz N., Warren D. Big Data. Principles and Practice of Building Scalable Data Processing Systems in Real Time. Moscow: Williams, 2016. (In Russ.)
4. Agibalov V. Iu. Virtual Traces in Forensics and Criminal Proceedings: Synopsis of a Thesis for a Candidate Degree in Law Sciences. Voronezh, 2010. (In Russ.)
5. Tsirin A. M., Cherepanova E. V., Tulinova O. A. Modern Standards and Technologies for Combating Corruption. *Journal of Russian Law*, 2014, no. 7. (In Russ.)
6. Gumarov I. A., Farakhiev D. M. Blockchain Technology as a Means of Combating Corruption. *Scientific Component*, 2022, no. 1 (13). (In Russ.)
7. Farakhiev D. M., Minzianova D. F. Transformation of the Subject and Method of Committing Crimes Under Articles 290 and 291 of the Criminal Code of the Russian Federation in the Process of Globalization. In *Novels of Law, Economics and Management 2022: Materials of the VIII International Scientific and Practical Conference, Gatchina, November 25, 2022. Vol. 1. Gatchina, 2023.* (In Russ.)
8. Farakhiev D. M. Activities of Economic Security and Anti-Corruption Units to Document Crimes Committed Using Digital Financial and Cryptocurrency Assets. *Works*

of the Academy of Management of the Ministry of Internal Affairs of Russia, 2023, no. 3 (67). (In Russ.)

9. Farakhiev D. M. Activities of Internal Affairs Bodies in the Process of Solving and Investigating Crimes Committed Using Information and Communication Technologies (Using Cryptocurrency Assets as an Example). *Legal Bulletin of Samara University*, 2023. Vol. 9, no. 3. (In Russ.)

Сведения об авторе:

Д. М. Фарахиев – адъюнкт.

Information about the author:

D. M. Farakhiev – Adjunct.

Статья поступила в редакцию 22.12.2025; одобрена после рецензирования 13.03.2025; принята к публикации 02.06.2025.

The article was submitted to the editorial office 22.12.2025; approved after reviewing 13.03.2025; accepted for publication 02.06.2025.