УДК: 35.086.2

Корнилов Анатолий Эдуардович
студент РЭУ имени Г.В. Плеханова,
Научный руководитель:
Лозовицкая Галина Петровна, доктор юридических наук,
профессор кафедры государственно-правовых и уголовно-правовых наук
РЭУ имени Г.В. Плеханова
E-mail: Lozovitskaya.GP@rea.ru

Уголовная ответственность за коррупционные преступления в цифровой экономике

Аннотация. Настоящее исследование посвящено выявлению особенностей уголовно-правовой ответственности за коррупционные преступления, совершаемые с опорой на цифровые инструменты и инфраструктуру. В работе показывается, что цифровизация одновременно обостряет классические коррупционные риски и предоставляет юридическому сообществу набор средств для их нейтрализации. Анализ норм главы 28 Уголовного кодекса Российской Федерации и сопоставимых международных актов демонстрирует необходимость обновления понятийного аппарата и санкционной системы под воздействием смарт-контрактов, криптоактивов и распределённых реестров. Автор приходит к выводу о том, что уголовно-правовой инструментарий уже содержит потенциал для адекватного реагирования, однако его применение требует методологического переосмысления и технологической подкреплённости государственными информационными платформами.

Ключевые слова: цифровая экономика, коррупция, смарт-контракт, криптоактив, уголовная ответственность, публичные закупки, блокчейн, прозрачность, УК РФ, профилактика.

Kornilov Anatoly Eduardovich,
student of Plekhanov Russian University of Economics,
Scientific supervisor:
Lozovitskaya Galina Petrovna, Doctor of Law, Professor of the Department of State Law and Criminal Law Sciences, Plekhanov Russian University of Economics

Criminal liability for corruption crimes in the digital economy

Abstract: This study explores the distinctive features of criminal liability for corruption offences committed with the aid of digital tools and infrastructure. It shows that digitalisation simultaneously heightens traditional corruption risks while equipping the legal community with new means to neutralise them. An analysis of Chapter 28 of the Criminal Code of the Russian Federation and comparable international instruments demonstrates the need to update both the conceptual framework and the system of sanctions in light of smart contracts, crypto-assets and distributed ledgers. The author concludes that existing criminal-law instruments already possess the potential for an adequate response; however, their application demands methodological rethinking and technological reinforcement via state information platforms.

Keywords: digital economy; corruption; smart contract; crypto-asset; criminal liability; public procurement; blockchain; transparency; Criminal Code of the Russian Federation; prevention.

Введение

За последние десять лет интенсивность цифровых трансформаций радикально изменила характер общественных отношений, породив феномен «цифровой коррупции» [2] — совокупности преступлений, в которых незаконная выгода извлекается посредством информационно-телекоммуникационных технологий. Российская статистика подтверждает, что

доля таких деяний растёт быстрее, чем общий массив экономической преступности, что ставит под сомнение устойчивость традиционных правовых механизмов противодействия. Одновременно государство внедряет цифровые сервисы судебного и административного контроля, сокращающие прямой контакт должностного лица и заявителя, тем самым снижая соблазн злоупотребления полномочиями. Возникает методологический парадокс: технологии, усиливающие прозрачность, в руках опытного преступника превращаются в средство сокрытия следов — прежде всего через шифрование транзакций, автоматизацию распределения средств и трансграничную мобильность данных [3].

Цели

Исследование направлено на формулирование комплексного подхода к квалификации и доказательству коррупционных преступлений, совершаемых в цифровой среде, а также на оценку эффективности действующих уголовно-правовых норм применительно к этим деяниям.

Задачи

Для достижения указанной цели автор, во-первых, анализирует эволюцию отечественного законодательства о преступлениях в сфере компьютерной информации и его корреляцию с антикоррупционными доктринами; во-вторых, сопоставляет российские уголовно-правовые решения с положениями Конвенции ООН против коррупции и зарубежными эмпирическими исследованиями; в-третьих, выявляет технологические векторы, требующие doctrinal fine-tuning при квалификации взяточничества, хищений и злоупотреблений, осуществляемых через цифровые платформы.

История проблемы

Российская правовая система традиционно воспринимала коррупцию через призму должностных злоупотреблений в офлайн-контексте. Первая волна цифровизации — внедрение федерального закона «Об информации, информационных технологиях и о защите информации» 2006 года — сместила фокус в сторону информационной безопасности, но не затронула

коррупционные схемы непосредственно. Второй этап, начавшийся после запуска национальной программы «Цифровая экономика», ознаменовался появлением специализированного блока уголовно-правовых норм о несанкционированном доступе к компьютерной информации и вредоносных программах, что, однако, лишь частично перекрыло возможности вывода активов через децентрализованные сети. Поворотным моментом стала Конвенция ООН против коррупции, задавшая трансграничный стандарт криминализации незаконного обогащения и восстановления активов, похищенных с применением высоких технологий.

Содержание и результаты исследования

Анализ главы 28 УК РФ [5] позволяет констатировать, что диспозиции, сконцентрированные на компьютерных данных как объекте посягательства, опосредованно защищают и экономические интересы государства. Однако они не охватывают сделки, где предметом выступают токенизированные активы или алгоритмические обременения, что создаёт лакуны при расследовании коррупционных схем с применением смарт-контрактов в сфере госзакупок. Публикации Серебренниковой и Трефилова[1] убеждают, что использование блокчейна в конкурсных процедурах способно блокировать манипуляции, но лишь при условии интеграции реестра с механизмами судебного контроля. Эмпирические данные Всемирного банка о манипулировании оценочными шкалами на аукционах показывают, что даже открытые электронные торги уязвимы, если алгоритм выставления баллов непрозрачен[9]. Российские материалы уголовных дел экономической направленности демонстрируют сходную картину: подавляющее большинство эпизодов связано с искаженными критериями отбора или подменой документации на портале закупок, что формально не попадает под квалификацию взяточничества, но приводит к тем же последствиям [11,12].

Документ ООН формулирует универсальные требования к криминализации подкупа в частном секторе и обращает особое внимание на возврат активов, перемещённых через цифровые каналы[10]. Сопоставление

этих положений с Указом Президента РФ № 478 о Национальном плане противодействия коррупции[4] показывает, что российская стратегия уже закрепила приоритет электронных сервисов мониторинга, однако не описала процедур верификации данных, поступающих из зарубежных блокчейн-сетей. Исследование цифровых антикоррупционных инструментов в различных правовых системах[7] фиксирует прямую зависимость между уровнем открытости госсервисов и снижением бытовой коррупции, при этом высокие показатели раскрытия данных не гарантируют уменьшения системных злоупотреблений, если программные компоненты не проходят регулярный аудит.

Российский пример единой информационной системы закупок иллюстрирует данный тезис[8]: платформа обеспечивает публичность тендерных процедур, но алгоритмы допуска подрядчиков к торгам всё ещё ограниченно верифицируются независимыми экспертами. Обобщение экономико-правовых исследований свидетельствует о том, что усиление санкций без одновременного повышения неизбежности выявления цифрового следа преступления не даёт статистически значимого эффекта[3]. Поэтому ключевым становится создание гибридной модели, сочетающей процессуальные гарантии цифрового доказательства (лог-файлы, хеш-суммы, метаданные распределённых реестров) и традиционные методы оперативно-розыскной работы. Расширение предмета взятки до нематериальных цифровых выгод — токенов доступа, привилегий в алгоритмах распределения трафика — требует уточнения диспозиций статей 290–291¹ УК РФ с учётом принципа правовой определённости.

Выводы

Цифровая экономика преобразовала как структуру коррупционных интересов, так и инструменты их пресечения. Действующее уголовное законодательство Российской Федерации обладает достаточным потенциалом для охвата большей части новых форматов преступлений, однако реализация этого потенциала зависит от своевременного методического переосмысления

понятий должностного подкупа, злоупотребления полномочиями и коммерческого подкупа применительно к нематериальным активам. Приоритетными направлениями совершенствования видятся разработка легального определения цифрового актива в контексте предмета взятки, внедрение обязательного технологического аудита алгоритмов госзакупок и создание межведомственной платформы обмена данными о транзакциях в распределённых реестрах с возможностью их использования в качестве судебного доказательства.

Список литературы

1. Serebrennikova A.V., Trefilov A.A. Criminal Anti-Corruption in the Era of Digital Technologies: The Russian Experience. Law: Journal of the University of Latvia. 2020.

2. Чернов С.Б. Противодействие коррупции в условиях цифровой экономики. Экономические науки. 2020.

3. Суходолов А.П., Колпакова Л.А., Спасенников Б.А. Проблемы противодействия преступности в сфере цифровой экономики. Всероссийский криминологический журнал. 2017.

4. Указ Президента РФ от 16.08.2021 № 478 «О Национальном плане противодействия коррупции на 2021–2024 годы».

5. Уголовный кодекс Российской Федерации. Глава 28 «Преступления в сфере компьютерной информации» (ред. 21.04.2025).

6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

7. Halai A. и др. Digital Anti-Corruption Tools and Their Implementation in Various Legal Systems Around the World. SHS Web of Conferences. 2021.

8. Egorova M. и др. Digitalization of Public Procurement in the Russian Federation: Case Study. The NISPAcee Journal of Public Administration and Policy. 2021.

9. Chen Q. Rigging the Scores: Corruption through Scoring Rule Manipulation in Public Procurement Auctions. World Bank, 2024.

10. United Nations Convention against Corruption. United Nations, 2004. (doaj.org, ResearchGate, КонсультантПлюс, КонсультантПлюс, mirnovskoe.rk.gov.ru, SHS Web of Conferences, Sciendo, unodc.org)

11. Уголовно-исполнительные, правовые, криминологические и оперативно-розыскные проблемы преступности в сфере экономики, влияющие на уголовную ответственность за легализацию активов организованной преступности / Г. П. Лозовицкая, А. В. Логинов, В. А. Минеев, Ю. В. Соколинский // Закон и власть. – 2025. – № 3. – С. 176-185. – EDN YVVQDX.

12. Лозовицкая, Г. П. Неочевидные ограничения режима совместного использования объекта интеллектуальных прав при исполнении законодательства о закупках для государственных и муниципальных нужд / Г. П. Лозовицкая, В. А. Минеев // Актуальные вопросы публично-правового регулирования экономических отношений : Материалы межвузовской научно-практической конференции, Москва, 21 декабря 2023 года. – Москва: ООО «РУСАЙНС», 2024. – С. 6-12. – EDN CKGWWV.