УДК 343.7

Акубекова Валентина Юрьевна
Студент, Высшая школа юриспруденции и судебно-технической экспертизы,
Санкт-Петербургский Политехнический университет,
РФ, г.Санкт-Петербург

ФИНАНСОВЫЕ ПРЕСТУПЛЕНИЯ В КИБЕРПРОСТРАНСТВЕ

Аннотация. С увеличением использования информационно-коммуникационных технологий, киберпреступность переживает бурное развитие, что делает её актуальной для правозащитников, исследователей и юристов. В настоящей статье особое внимание уделяется налоговым преступлениям, которые служат способом сокрытия доходов, полученных от незаконной деятельности, так как эти действия наносят ущерб не только экономике государства, но и социально-экономическому равновесию в обществе в целом. На настоящий момент на международном уровне нет единой дефиниции финансовых преступлений, что затрудняет борьбу с ними. В данной статье рассматриваются определения данного преступления, и этот анализ позволяет выявить основные подходы к классификации финансовых преступлений и осветить пробелы в рамках функционирующего законодательства. Статья поднимает важный вопрос о налоговых преступлениях, связанных с сокрытием доходов от незаконной деятельности, и внимание к этой теме обусловлено актуальностью проблем, возникающих в условиях быстрого развития технологий и цифровизации финансовых операций, и основная цель написания работы заключается в анализе способов, которыми преступники используют киберпространство для уклонения от уплаты налогов, а также в разработке методов их выявления и предотвращения. Для достижения поставленных целей в исследовании была применена методология, включающая как теоретический, так и практический подходы. Теоретическая часть основывается на анализе существующего

законодательства, исторических данных и международных стандартов, связанных с кибербезопасностью и борьбой с финансовыми преступлениями, а практический аспект исследования включает изучение реальных кейсов финансовых преступлений в киберпространстве, а также вмешательства правоохранительных органов и эффективность их методов в борьбе с подобными правонарушениями. Результаты работы могут быть использованы для формирования стратегий и подходов к борьбе с финансовыми преступлениями. Социальная опасность и сложность финансовых преступлений, рассматриваемых в этой статье, требуют их выделения как особого вида преступлений в законодательстве, что позволит преследовать виновных лиц и предотвращать подобные действия в будущем. Основной акцент на социальную опасность этих преступлений подчеркивает необходимость более активного участия как государственных органов, так и общества в противодействии киберпреступности.

Ключевые слова: квалификация преступлений, финансовое преступление, киберпреступление, киберпространство, налоговые преступления, доходы от незаконной деятельности.

With the increasing use of information and communication technologies, cybercrime is experiencing rapid development, which makes it relevant for human rights defenders, researchers and lawyers. In this article, special attention is paid to tax crimes, which serve as a way to conceal income received from illegal activities, since these actions damage not only the economy of the state, but also the socio-economic balance in society as a whole. At the moment, there is no single definition of financial crimes at the international level, which makes it difficult to combat them. This article examines the definitions of this crime, and this analysis allows us to identify the main approaches to classifying financial crimes and highlight gaps in the framework of functioning legislation. The article raises an important issue about tax crimes related to the concealment of income from illegal activities, and attention to this topic is due to the urgency of the problems that arise in the context of the

rapid development of technology and digitalization of financial transactions, and the main purpose of writing this work is to analyze the ways that criminals use cyberspace to evade taxes, as well as to develop methods of their detection and prevention. To achieve these goals, the research applied a methodology that includes both theoretical and practical approaches. The theoretical part is based on an analysis of existing legislation, historical data and international standards related to cybersecurity and combating financial crimes, while the practical aspect of the study includes the study of real cases of financial crimes in cyberspace, as well as the intervention of law enforcement agencies and the effectiveness of their methods in combating such offenses. The results of the work can be used to form strategies and approaches to combating financial crimes. The social danger and complexity of financial crimes discussed in this article require their identification as a special type of crime in the legislation, which will make it possible to prosecute the perpetrators and prevent similar actions in the future. The focus on the social danger of these crimes highlights the need for more active involvement of both government agencies and society in countering cybercrime.

Keywords: qualification of crimes, financial crime, cybercrime, cyberspace, tax crimes, income from illegal activities.

Финансовые преступления в киберпространстве представляют собой проблемный феномен как с точки зрения теории, так и практики (в первую очередь расследования), который стал предметом активного исследования, для надлежащего применения уголовного законодательства в отношении виновных лиц необходимо понимать сущность совершённого акта, его мотивацию и цели применения закона, так как именно это понимание лежит в основе квалификации финансовых преступлений, с которыми юристы-практики и исследователи-теоретики сталкиваются в ходе своей деятельности.

Отсутствие единой и общепринятой дефиниции киберпреступности создает трудности как для правоприменения, так и для теоретического осмысления этого явления. Киберпреступность охватывает широкий спектр действий,

которые могут быть виртуальным или реальным результатом преступной деятельности, осуществленной в цифровом пространстве, и распространённая классификация преступлений по различным признакам (таким как объект правовой защиты или способ совершения преступления) приводит к неоднозначности и даже дублированию. Это становится особенно заметным, когда речь идет о преступлениях, которые невозможно разделить по простому критерию их осуществления или содержания, например, такие явления, как фишинг или кибертерроризм, затрагивают несколько категорий преступлений одновременно, что требует от юридических систем большей гибкости и точности в определении соответствующих норм.

Одним из главных документов в этой области стала Конвенция Совета Европы о киберпреступности, однако представленная в ней классификация киберпреступлений также не является исчерпывающей из-за отсутствия единого критерия для разграничения преступлений, что приводит к ситуации, когда одни и те же действия квалифицируются по-разному в зависимости от правовой системы конкретной страны и наличия законодательных актов, которые могли бы охватывать новые технологии и методы совершения преступлений. В контексте Конвенции Совета Европы по киберпреступности[1] выделяются важные категории преступлений, такие как нарушения конфиденциальности и целостности данных, но, как вы отметили, отсутствие единого критерия усложняет правоприменение. Отдельной темой в этом контексте являются финансовые преступления, включая налоговые преступления в целях сокрытия доходов от незаконной деятельности, которые в значительной степени зависят от киберпространства, ведь их масштабы и многообразие схематических атак и манипуляций только увеличиваются с прогрессом технологий. Сложные схемы отмывания денег, мошенничества и других финансовых преступлений становятся изощрённей и труднее для выявления и преследования.

[1] The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005 // URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата обращения: 14.05.2025).

Уклонение от уплаты налогов и отмывание денег имеют долгую историю, и их признание взаимосвязанными преступлениями открыло новые перспективы для практики правоприменения. Признание проблемой уклонения от уплаты налогов через дело Аль Капоне (который был осуждён именно за это, а не за создание мафиозной группировки) символизирует начало активного применения законодательства в данной области, что стало важным моментом, поскольку сложность финансовых преступлений требовала создания четких механизмов для их преследования. С течением времени, в ответ на глобализацию и развитие технологий, которое сделало возможным не только укрытие доходов, но и их дальнейшее отмывание, законодательные инициативы начали активнее разрабатываться. Концепция предикатных преступлений, заимствованная из американского законодательства, является ключевой для понимания этого вопроса, размеры и методы уклонения от уплаты налогов, используя киберпространство, требует от государств переосмысления существующих норм. Концепция предикатных преступлений помогает увидеть, как различные преступления, такие как мошенничество с налогами и отмывание денег, могут быть связаны через криминальные доходы. В существующих в Уголовном кодексе РФ статьях закреплены составы преступления, связанные с сокрытием денежных средств или иных активов, выступающими объектами налогообложения для юридических лиц и индивидуальных предпринимателей (ст. 199.2). Кроме того, закреплены и положения, определяющие уголовную ответственность за неисполнение обязанностей налогового агента (ст. 199.1)[2]. Однако следует указать, что в составе указанных преступлений отсутствуют признаки налоговых преступлений, которые могут быть совершены в киберпространстве, то есть сложность киберналоговых преступлений в том, что многие страны по-прежнему используют традиционный подход к налогообложению и правоприменению, что неадекватно текущей реальности,

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025) // Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954.

глобализация преступных действий не оставляет выбора: страны должны усовершенствовать законодательные подходы, сотрудничать на международном уровне.

Отсутствие явных признаков налоговых преступлений в киберпространстве в российском законодательстве, безусловно, является проблемой. Налоговое законодательство должно учитывать не только традиционные способы уклонения от уплаты налогов, но и новые сценарии, возникшие в результате цифровой трансформации. Специализированные подходы к правоприменению, включая использование технологий, таких как блокчейн для отслеживания транзакций, становятся необходимыми элементами в борьбе с этими актуальными видами преступлений. Среди множества финансовых преступлений, которые совершаются в киберпространстве, отмывание денег и налоговые преступления занимают особое место из-за своего распространения и внедрения разнообразных методов легализации незаконно полученных доходов. С развитием Интернета возросла обеспокоенность по поводу конфиденциальности пользователей, что стало одной из причин для разработки криптографических методов для защиты личной информации, и заметной из этих технологий выступает криптография с открытым ключом, которая позволяет скрыть содержание передаваемой информации для всех, кто не является участником определенной системы, данная технология лежит в основе блокчейн-технологии и, соответственно, криптовалют, которые часто используются для уклонения от уплаты налогов, скрывая личности участников незаконных операций, таких как отмывание средств.

Электронные переводы, в том числе с использованием криптовалют, упрощают процесс сокрытия активов в оффшорах. В отличие от традиционных методов, которые требовали физического перемещения средств, кибертехнологии позволяют физическим лицам в одной стране управлять оффшорными счетами, не выходя из дома. Более того, технологии киберпространства способствуют налоговой практике, позволяющей частным

лицам и компаниям перемещать налогооблагаемую прибыль из юрисдикций с высокими налогами в юрисдикции с низкими налогами, то есть новые методы использования киберпространства помогают компаниям минимизировать налоговые обязательства, размещая нематериальные активы, пользователей и серверы в различных юрисдикциях.

Важным аспектом является то, что большинство технологических изменений начинается с процесса «оцифровки» – преобразования информации в цифровой формат, что привело к тому, что многие аспекты повседневной жизни становятся частью этого нового киберпространства, т.е. всё больше сторон жизни охватывает такое явление, как «цифровизация». В результате появляются новые. технологии, такие как электронные наличные, электронная торговля, блокчейн и одноранговые сети, которые, в свою очередь, также содействуют правонарушениям в области налогообложения. Со времени появления наличных денег, которые долгое время были основным средством ведения экономических транзакций и облегчили уклонение от уплаты налогов из-за своей анонимности, сегодня наблюдается тенденция их вытеснения более современными формами, такими как кредитные и дебетовые карты, а также платежные приложения. Несмотря на то, что эти новые формы позволяют отслеживать денежные потоки, криминальные элементы находят способы их обхода, используя технологии для совершения незаконных электронных транзакций. Технология блокчейн, представляющая собой децентрализованную систему учета транзакций, обеспечивает высокую степень защищенности от несанкционированного доступа и дают возможность осуществлять транзакции без необходимости третьих сторон. Другим вызовом для налоговых поступлений становится система цепочек поставок, которая представляет собой комплекс взаимодействий между людьми, видами деятельности, ресурсами и организациями, способствующих перемещению товаров от производителей к потребителям, так как глобальные компании (в том числе преступные организации) с легкостью могут «распределять» свои производственные мощности в различных юрисдикциях,

что дает им возможность манипулировать ценами и минимизировать налоговые обязательства через трансфертное ценообразование.

Одноранговые сети (P2P) также вносят изменения в традиционные отношения между поставщиками и потребителями[3], позволяя им напрямую взаимодействовать через цифровые платформы, - этот новый формат трансакций подразумевает одноразовые отношения между сторонами, что также создает трудности в налогообложении; фактически, такие платформы позволяют участникам рынка обходить налоговую систему, что еще больше усложняет правоприменение и сбор налогов.

Итак, рассматривая трансграничный характер финансовых преступлений, следует подчеркнуть, что использование интернет-технологий создает новые пути для мошенничества и отмывания денег; - преступные схемы, часто связанные с онлайн-платежами и работой виртуальных казино, становились всё изощрённее, что требует от правоохранительных органов новых подходов и методов противодействия, и барьером в борьбе с такими преступлениями является также активное использование той или иной виртуальной валюты; отсутствие четких законодательных норм и детального регулирования этой сферы создаёт идеальные условия для уклонения от уплаты налогов и легализации денежных средств, полученных преступным путем. Финансовые преступления в киберпространстве имеют далеко идущие последствия как для отдельной личности, так и для общества в целом, а потому необходимо наращивать усилия в области правоприменения, подготовки кадров и разработки новых законодательных инициатив, направленных на борьбу с киберпреступностью и защиту правопорядка.

Список источников

1. The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005 // URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата обращения: 14.05.2025).

[3] Гладыч Н.В. Налоговые преступления в киберпространстве: проблемы квалификации// Вопросы российского и международного права. 2021. Том 11. № 11А. С. 149-155.

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025) // Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954.

3. Гладыч Н.В. Налоговые преступления в киберпространстве: проблемы квалификации// Вопросы российского и международного права. 2021. Том 11. № 11А. С. 149-155.