Криминологическое противодействие экономическим преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий

Ирина Сергеевна МОЧАЛКИНА,
преподаватель кафедры криминологии и уголовно-исполнительного права, заместитель директора Института публичного права и управления Университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук
ismochalkina@msal.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Аннотация. *В статье анализируются новые средства и способы совершения экономических преступлений в эпоху цифровизации. Автор исследует новые способы совершения преступлений при покупке, продаже товаров на маркетплейсах и приходит к выводу, что основными мерами предупреждения экономических преступлений в условиях цифровой экономики являются совершение платежей на интернет-ресурсах с отдельной банковской карты, на которой находится небольшая денежная сумма; игнорирование пользователем сторонних ссылок в момент осуществления покупок на сайте маркетплейса. При этом в случае технического сбоя на маркетплейсе, в результате которого пользователь без оплаты приобретает товары, лицо подлежит уголовной ответственности. В статье обращается внимание на распространение использования технологии дипфейк при осуществлении хищения денежных средств, предлагается в целях предупреждения таких преступлений поддержать законопроект, согласно которому необходимо установить квалифицирующие признаки в ст. 158 и ст. 159 УК РФ, предполагающие совершение преступления с использованием подмены признаков личности. Автор приходит к выводу, что введение в гражданский оборот цифрового рубля и внесение изменений в отдельные постановления Пленума Верховного Суда РФ в части признания криптовалюты объектом хищения поможет снизить уровень некоторых экономических преступлений.*

Ключевые слова: *дипфейк, криптовалюта, цифровой рубль, виртуальные активы, киберпреступление, блокчейн, фишинг, хищение*

DOI: 10.17803/2311-5998.2025.129.5.189-196

Irina S. MOCHALKINA,
Lecturer of the Department of Criminology and Criminal-Executive Law, Deputy Director of the Institute of Public Law and Management of the Kutafin Moscow State Law University (MSAL), Cand. Sci. (Law)
ismochalkina@msal.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Criminological counteraction to economic crimes committed using information and telecommunication technologies

Abstract. *The article analyzes new means and methods of committing economic crimes in the digital era. The author examines new ways of committing crimes when buying and selling goods on marketplaces and comes to the conclusion that the main measures to prevent economic crimes in the digital economy are making payments on Internet resources from a separate bank card with a small amount of money; ignoring third-party links by the user when making purchases on the marketplace website. At the same time, in the event of a technical failure on the marketplace, as a result of which the user purchases goods without payment, the person is subject to criminal liability. The article draws attention to the widespread use of deepfake technology in theft of funds, and proposes to support the bill in order to prevent such crimes, according to which it is necessary to establish qualifying features in Art. 158 and Art. 159 of the Criminal Code of the Russian Federation, which involve committing a crime using the substitution of personality traits. The author concludes that the introduction of the digital ruble into civil circulation and amendments to certain Resolutions of the Plenum of the Supreme Court of the Russian Federation in terms of recognizing cryptocurrency as an object of theft will help reduce the level of certain economic crimes.*
Keywords: *deepfake, cryptocurrency, digital ruble, virtual assets, cybercrime, blockchain, phishing, theft*

Согласно отчету МВД РФ о состоянии преступности в Российской Федерации за январь — декабрь 2024 г., за указанный период было зарегистрировано 765,4 тыс. преступлений, совершенных с использованием высоких технологий, что на 13,1 % больше, чем в 2023 г. Удельный вес преступлений, совершенных при помощи информационно-телекоммуникационных технологий, в общем числе зарегистрированных преступлений составил 40 %, что указывает на рост преступлений в цифровой среде[1]. Стóит отметить, что около половины таких деяний относятся к категориям тяжких и особо тяжких преступлений;

[1] Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2024 года // URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 25.03.2025).

с использованием сети Интернет совершались 4 преступления из 5. При этом две трети указанных преступлений (63,5 %) составили кражи и мошенничества.

По заявлению Президента РФ, ущерб от киберпреступлений в 2024 г. составил около 200 млрд рублей, уровень раскрываемости преступлений в сфере информационно-телекоммуникационных технологий снизился, но при этом злоумышленники находят новые способы совершения преступлений[2]. Вышесказанное обусловливает необходимость изучения и разработки мер противодействия экономическим преступлениям, совершенным с использованием цифровых инструментов.

Согласно оценкам аналитиков больше 3 млрд записей, которые содержат персональные данные людей, находятся в открытом доступе в сети Интернет, при этом в большинстве случаев источниками утечки информации являются не банки и финансовые организации[3]. Например, в 2024 г. была организована крупнейшая кибератака на государственную систему, использующуюся для управления судебными процессами, — ГАС «Правосудие». Злоумышленники получили информацию о состоянии судебных дел граждан, а также персональные данные лиц, участвующих в процессах.

Зачастую пользователи сети Интернет собственноручно вручают данные о себе представителям криминального мира при регистрации на маркетплейсах и иных ресурсах, которые плохо защищены. Нередко, получив логин и пароль от входа в личный кабинет маркетплейса, мошенники совершают у подконтрольных лиц множество покупок на сумму, не превышающую 1 000 руб. для обхода ввода кода подтверждения от банка, после чего полученные денежные средства выводят. При покупке товаров в сети Интернет существуют и иные уловки недобросовестных продавцов: создание фишинговых сайтов, которые визуально трудно отличимы от официальных; появление всплывающего окна со скидкой в момент совершения покупки на сайте, при клике на которое злоумышленнику передаются банковские данные пользователя.

Вместе с тем не только продавцы, но и покупатели маркетплейсов могут являться субъектом совершения экономических преступлений в эпоху цифровизации. Так, в 2024 г. 23-летняя жительница Красноярска зарегистрировала аккаунт на Wildberries, далее при добавлении товаров в корзину она обнаружила технический сбой. Все товары, выбранные покупателем, автоматически приобретали статус «оплачено». Заметив данный факт, девушка не сообщила о сбое в службу поддержки, а продолжила совершать покупки различных товаров, в том числе смартфоны, золотые украшения. Общая сумма покупок злоумышленницы составила 1,2 млн руб., после чего приобретенные товары были выставлены ею на продажу в других магазинах[4]. Прокуратура утвердила обвинение в мошенничестве в особо крупном размере.

---

[2] Ущерб от киберпреступлений в 2024 году составил порядка 200 млрд рублей // URL: https://www.kommersant.ru/doc/7552645 (дата обращения: 25.03.2025).

[3] Действия мошенников в Интернете в 2024 году обойдутся в 1 трлн рублей // URL: https://www.vedomosti.ru/technology/articles/2024/11/06/1073370-deistviya-moshennikov-1-trln (дата обращения: 25.03.2025).

[4] В Красноярске женщина обманула Wildberries на 1,2 миллиона рублей // URL: https://ria.ru/20241021/wildberries-1979117404.html (дата обращения: 25.03.2025).

Рассмотренный случай не является единичным. В 2024 г. к уголовной ответственности был привлечен житель Крыма, который из-за технического сбоя приобрел без оплаты товары на маркетплейсе на сумму свыше 13 млн руб. Суд приговорил злоумышленника к 4 годам колонии общего режима со штрафом в 130 тыс. руб.[5]

Для анализа и изучения интересен вопрос, связанный со снижением стоимости товара на маркетплейсе в случае технического сбоя или по иным причинам, его последующей покупкой пользователем маркетплейса и необходимостью привлечения покупателя к ответственности. Согласно определению Верховного Суда РФ от 04.04.2023 № 49-КГ22-28-К6, в 2021 г. на сайте ООО «Сеть Связной» пользователь дистанционным способом приобрел телевизор, уплатив за него 480 руб.[6] При оформлении заказа была определена дата доставки товара, но в этот день покупатель не получил телевизор, а уплаченные денежные средства были возвращены пользователю сайта. Несмотря на заниженную почти в 80 раз стоимость товара, суд пришел к выводу, что магазин не вправе отказаться от передачи оплаченного товара. В рассматриваемом случае покупатель действовал правомерно, требуя доставки купленного товара за 480 руб. в определенные сторонами сроки; в его действиях не содержатся признаки состава преступления.

В качестве основных мер предупреждения экономических преступлений, совершаемых при покупке и продаже товаров на маркетплейсах, можно выделить следующие: совершение платежей на интернет-ресурсах с отдельной банковской карты, на которой находится небольшая денежная сумма; отключение опции «сохранение пароля и логина» на сайте маркетплейса; проверка рейтинга продавца; игнорирование пользователем сторонних ссылок в момент осуществления покупок на сайте маркетплейса; периодическая смена пароля покупателем; совершение покупок через защищенную домашнюю сеть вместо открытых сетей Wi-Fi, поскольку с помощью анализатора трафика можно получить данные для входа на некоторые сайты, используемые жертвой.

Развитие компьютерных технологий привело к созданию на основе образцов голоса и изображения человека видео-, аудиоматериалов, иллюстрирующих несуществующие события, явления и процессы, — дипфейков. В настоящее время отличить оригинальное видеоизображение лица от сконструированного искусственным интеллектом зачастую не представляется возможным без привлечения специалиста. Несколько лет назад мошенники из Гонконга, используя технологию дипфейк, смогли похитить 26 млн долларов у крупной корпорации, позвонив по видеосвязи сотрудникам, выдав себя за старшего менеджера компании и попросив перевести денежные средства на банковский счет[7].

---

[5] Житель Крыма обманул маркетплейс на 13 млн рублей // URL: https://crimea.ria.ru/20241029/zhitel-kryma-obmanul-marketpleys-na-13-mln-rubley-1141452360.html (дата обращения: 20.03.2025).

[6] Определение Верховного Суда РФ № 49-КГ22-28-К6 от 04.04.2023 // URL: https://ur29.ru/resheniya-sudov/vsrf-49-kg22-28-k6-ot-04042023/ (дата обращения: 20.03.2025).

[7] В Гонконге с помощью дипфейка украли миллионы долларов у крупнейшей корпорации // URL: https://rg.ru/2024/02/04/v-gonkonge-s-pomoshchiu-dipfejka-moshenniki-ukrali-milliony-dollarov-u-krupnejshej-korporacii.html (дата обращения: 15.03.2025).

Сегодня одной из распространенных схем мошенничества с использованием дипфейков является фейковый розыгрыш денежных средств среди подписчиков в социальной сети блогера, которая предварительно взламывается злоумышленником. На основе опубликованных автором оригинальных аудио-, фото-, видеоматериалов преступник создает дипфейк с просьбой к подписчикам поучаствовать в конкурсе, для чего необходимо перейти по ссылке на определенный сайт. После совершения описанного действия жертве приходит сообщение о выигрыше, для получения которого необходимо заплатить комиссию. Так, один из самых популярных YouTube-блогеров MrBeast, имеющий более 300 млн подписчиков, опубликовал в своей социальной сети в 2023 г. информацию о том, что мошенники при помощи нейросетей создали фейковое видео, в рамках которого он призывает к участию в конкурсе, а для получения выигрыша пользователю необходимо зайти на специальный сайт и оплатить комиссию[8]. При переходе по ссылке подписчики не только оплачивали необходимый взнос, но и лишались гораздо более крупных денежных сумм в результате проведенной транзакции. Сто́ит отметить, что описанная схема мошенничества распространена и на территории нашей страны.

В целях противодействия преступлениям, совершаемым с использованием технологии дипфейк, в 2024 г. в Государственную Думу был внесен законопроект, в котором предлагалось внести в УК РФ изменения, в частности, в ст. 158 и 159 УК РФ, дополнив их квалифицирующими признаками: «*с использованием изображения или голоса (в том числе фальсифицированных или искусственно созданных) потерпевшего или иного лица, а равно с использованием биометрических персональных данных потерпевшего или иного лица*»[9]. За совершение мошенничества с использованием рассматриваемой технологии законопроектом предусмотрено самое строгое наказание в виде лишения свободы на срок до шести лет.

Несмотря на имеющуюся в настоящее время возможность квалификации содеянного по действующим нормам УК РФ, представляется, что введение квалифицирующего признака в статьях, регламентирующих хищения, будет являться сдерживающим фактором для злоумышленников из-за усиления уголовной ответственности. Однако прежде чем устанавливать уголовную ответственность, в рамках отраслевого законодательства необходимо урегулировать правовое положение и вопросы использования технологий подмены признаков личности.

При совершении хищений в информационно-телекоммуникационной сети злоумышленники используют не только технологию дипфейк, но и новые методы посягательства на криптовалюту. По данным аналитической компании Chainalysis, общая сумма хищений указанного виртуального актива за 2024 г. киберпреступниками составила свыше 2,2 млрд долларов, что больше на 21 % по сравнению с 2023 г.[10]

[8] MrBeast разоблачает мошенничество с дипфейками // URL: https://www.cryptopolitan.com/ru/mrbeast-exposes-deepfake-scam/ (дата обращения: 18.03.2025).

[9] Законопроект № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации» // URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 18.03.2025).

[10] В 2024 году хакеры украли криптовалюту на $ 2,2 млрд // URL: https://www.kommersant.ru/doc/7399554 (дата обращения: 10.03.2025).

Одной из новых схем совершения хищения, предметом которого выступает криптовалюта, является привлечение злоумышленниками к завладению цифровыми активами иных представителей преступного мира. Так, притворяясь неопытными пользователями криптовалют, преступники в социальных сетях или тематических чатах пишут сообщения, в которых просят помочь вывести криптовалюту с цифрового кошелька, а также указывают определенную фразу, которая служит ключом доступа к хранилищу.

Данная схема рассчитана на тех пользователей, которые решат воспользоваться оставленным в сообщении ключом и вывести чужую криптовалюту на свой криптовалютный кошелек. При вводе ключа пользователь замечает, что для оплаты комиссии за осуществление транзакции на кошельке отсутствует необходимая сумма, после чего он переводит необходимые средства на адрес криптовалютного кошелька, но комиссия уходит на другой адрес, подконтрольный злоумышленнику. В настоящее время с такими сообщениями пользователи все чаще сталкиваются на Youtube и Telegram, модераторы которых в целях предупреждения хищений денежных средств стараются оперативно удалять подобные комментарии.

Новым способом совершения хищений, предметом которых выступает криптовалюта, является рассылка приглашений в фейковые видеоконференции Zoom. После того как пользователь перейдет по ссылке и нажмет «начать конференцию», на его устройство устанавливается вредоносное программное обеспечение, которое позволяет получить множество данных о человеке, в том числе ключи от криптовалютных кошельков. Собранная информация о пользователе передается на сервера, подконтрольные злоумышленникам. Поскольку возбуждение уголовных дел по факту хищения криптовалюты во многих случаях затруднительно и вызывает вопросы, что создает простор для дальнейшей деятельности злоумышленников, предлагается внести изменения в постановления Пленума Верховного Суда РФ о судебной практике по делам о мошенничестве, присвоении и растрате, краже, грабеже и разбое и признать криптовалюту предметом хищений.

Еще одним инструментом противодействия экономическим преступлениям является введение в гражданский оборот цифрового рубля, который в 2023 г. был включен в ст. 128 ГК РФ в перечень объектов гражданских прав. Цифровые рубли представляют собой третью форму национальной валюты, среди них могут появиться такие средства платежа, которые позволят определять его назначение. В частности, в рамках бюджетного финансирования государством могут быть выделены цифровые рубли для выполнения каких-либо работ или оказания услуг, которые будет невозможно израсходовать иным образом, кроме целевого назначения. В случае попытки перевода цифровых рублей не по корректному платежному адресу система не позволит выполнить транзакцию. Таким образом, цифровой рубль является новым инструментом противодействия финансовым, коррупционным преступлениям, который активно тестируется в настоящее время в целях его дальнейшего запуска на территории Российской Федерации.

Вместе с тем хищение цифрового рубля также становится затруднительным. Взлом блокчейна, на основе которого будет функционировать цифровой рубль, теоретически возможен, но на практике маловероятен. Самая большая проблема в данном случае будет заключаться в методах социальной инженерии, которые

повсеместно используются мошенниками. Например, злоумышленник в телефонном звонке может представиться сотрудником Центробанка и попросить пользователя перевести цифровой рубль на другой цифровой кошелек. Одной из основных мер предупреждения таких хищений является систематическое информирование граждан о новых средствах платежа, принципах их функционирования, запрете передачи данных от входа в цифровой кошелек.

Таким образом, среди основных мер противодействия экономическим преступлениям, совершаемым при покупке и продаже товаров на маркетплейсе с использованием технологии дипфейк и новых методов получения ключей от криптовалютных кошельков, можно выделить следующие:

1) совершение платежей на интернет-ресурсах с отдельной банковской карты, на которой находится небольшая денежная сумма;
2) отключение опции «сохранение пароля и логина» на сайте маркетплейса;
3) проверка рейтинга продавца;
4) игнорирование пользователем сторонних ссылок в момент осуществления покупок на сайте маркетплейса;
5) периодическая смена пароля покупателем;
6) совершение покупок через защищенную домашнюю сеть вместо открытых сетей Wi-Fi;
7) введение квалифицирующего признака в статьях, регламентирующих хищения, в рамках которого будет предусмотрена повышенная уголовная ответственность за использование технологии дипфейк;
8) введение в гражданский оборот цифрового рубля;
9) повышение уровня правового сознания граждан, систематическое информирование общества о новых средствах платежа.

БИБЛИОГРАФИЯ

1. В 2024 году хакеры украли криптовалюту на $2,2 млрд // URL: https://www.kommersant.ru/doc/7399554 (дата обращения: 10.03.2025).
2. В Гонконге с помощью дипфейка украли миллионы долларов у крупнейшей корпорации // URL: https://rg.ru/2024/02/04/v-gonkonge-s-pomoshchiu-dipfejka-moshenniki-ukrali-milliony-dollarov-u-krupnejshej-korporacii.html (дата обращения: 15.03.2025).
3. В Красноярске женщина обманула Wildberries на 1,2 миллиона рублей // URL: https://ria.ru/20241021/wildberries-1979117404.html (дата обращения: 25.03.2025).
4. Действия мошенников в интернете в 2024 году обойдутся в 1 трлн рублей // URL: https://www.vedomosti.ru/technology/articles/2024/11/06/1073370-deistviya-moshennikov-1-trln (дата обращения: 25.03.2025).
5. Житель Крыма обманул маркетплейс на 13 млн рублей // URL: https://crimea.ria.ru/20241029/zhitel-kryma-obmanul-marketpleys-na-13-mln-rubley-1141452360.html (дата обращения: 20.03.2025).
6. Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2024 года // URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 25.03.2025).

7. Ущерб от киберпреступлений в 2024 году составил порядка 200 млрд рублей // URL: https://www.kommersant.ru/doc/7552645 (дата обращения: 25.03.2025).
8. MrBeast разоблачает мошенничество с дипфейками // URL: https://www.cryptopolitan.com/ru/mrbeast-exposes-deepfake-scam/ (дата обращения: 18.03.2025).