УДК 343.72
ББК 67.408.121.2

МОШЕННИЧЕСКИЕ ПРОЯВЛЕНИЯ ФЕЙКОВ И ДИПФЕЙКОВ: ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ

Ю. Ю. Малышева

Всероссийский государственный университет юстиции (РПА Минюста России) (Казань, Россия)

Цифровые технологии открыли путь фейковым преступлениям. Одним из наиболее популярных преступлений в сфере цифровых технологий является мошенничество в цифровом поле, отличающееся традиционным способом его совершения — обмана, но которое приобрело новые черты и схемы в эпоху цифровой трансформации. В современных реалиях мошенничество можно считать классическим примером «фейкового» преступления, поскольку в его основе лежит обман как неотъемлемый способ его совершения.

Цифровая трансформация вывела 2023 г. на рекордное количество преступлений в сфере цифровых технологий: по официальной статистике МВД России более 677 тыс. IT-преступлений. В 2022 г. настоящие показатели были на треть меньше, или равнялись 522 тыс. подобных преступлений.

В 2023 г. удельный вес преступлений в сфере цифровых технологий вырос до 34,8% по сравнению с 2022 г., когда удельный вес подобных преступлений составлял 26,5%. Более половины зарегистрированных преступлений, совершенных с помощью информационных технологий, относятся к категориям тяжких и особо тяжких.

За 2023 г. по сравнению с предыдущим годом больше всего в абсолютном выражении выросло количество преступлений, совершенных с использованием сети Интернет. Показатели выросли с 381,1 до 526,7 тыс. Примечательно, что на втором и третьем местах оказалось мошенничество, совершенное с применением средств мобильной связи и пластиковых карт. Также в цифровом пространстве участились фейковые преступления с использованием компьютерной техники, программных средств и фиктивных электронных платежей.

Ключевые слова: мошенничество как фейковое преступление, фейки в уголовном праве, уголовная ответственность за дипфейки

FRAUDULENT MANIFESTATIONS OF FAKES AND DEEPFAKES: PROBLEMS OF COUNTERACTION

Yu. Yu. Malysheva

All-Russian State University of Justice (RPA of the Ministry of Justice of Russia) (Kazan, Russia)

Digital technologies have paved the way for fake crimes. One of the most popular crimes in the field of digital technologies is digital fraud, which is distinguished by the traditional method of deception, but which has acquired new features and patterns in the era of digital transformation. In modern realities, fraud can be considered a classic example of a «fake» crime, since it is based on deception as an integral way of committing it.

Digital transformation has brought 2023 to a record number of digital crimes. According to official statistics of the Russian Ministry of Internal Affairs, there are more than 677,000 IT crimes. Compared to 2022, the actual figures were a third lower, or equal to 522,000 such crimes.

In 2023, the share of digital crimes increased to 34.8% compared to 2022, when the share of such crimes was 26.5%. More than half of the registered crimes committed with the help of information technologies belong to the categories of grave and especially grave.

In 2023, compared to the previous year, the number of crimes committed using the Internet increased the most in absolute terms. The figures increased from 381.1 thousand to 526.7 thousand. It is noteworthy that in second and third places were fraud committed using mobile communications and plastic cards. Also

in the digital space, fake crimes using computer equipment, software and fictitious electronic payments have become more frequent.

Keywords: fraud as a fake crime, fakes in criminal law, criminal liability for deepfakes

Doi: https://doi.org/10.14258/ralj(2025)1.16

Тема цифровой трансформации отличается особой актуальностью и удобством в современных реалиях, но нельзя не отметить и «ложку дегтя» в привычной повседневной жизни успешного пользователя цифровыми технологиями.

Цифровые технологии открыли путь фейковым преступлениям. Одним из наиболее популярных преступлений в сфере цифровых технологий является мошенничество в цифровом поле, которое приобрело новые черты и схемы именно в эпоху цифровой трансформации. В современных реалиях мошенничество можно считать классическим примером фейкового преступления, поскольку в его основе лежит обман как неотъемлемый способ его совершения [1, с. 72].

Цифровая трансформация вывела 2023 г. на рекордное количество преступлений в сфере цифровых технологий: по официальной статистике МВД России более 677 тыс. IT-преступлений. В 2022 г. настоящие показатели были на треть меньше: 522 тыс. подобных преступлений.

В 2023 г. удельный вес преступлений в сфере цифровых технологий вырос до 34,8% по сравнению с 2022 г., когда удельный вес подобных преступлений составлял 26,5%. Более половины зарегистрированных преступлений, совершенных с помощью информационных технологий, относятся к категориям тяжких и особо тяжких.

За 2023 г. по сравнению с предыдущим годом больше всего в абсолютном выражении выросло количество преступлений, совершенных с использованием сети Интернет. Показатели выросли с 381,1 до 526,7 тыс. Примечательно, что на втором и третьем местах оказалось мошенничество, совершенное с применением средств мобильной связи и пластиковых карт. Также в цифровом пространстве участились преступления с использованием компьютерной техники, программных средств и фиктивных электронных платежей [2, с. 27].

По словам представителей МВД по Республике Татарстан, за 9 месяцев 2024 г. в отделах полиции Татарстана зарегистрировано больше 25 тыс. заявлений о преступлениях в сфере информационных технологий. Это почти на 45% больше, чем в 2023 г.

Значительный прирост преступлений, совершенных в сфере цифровых технологий, статистикой МВД отмечен в Ненецком автономном округе, Калмыкии, Новгородской и Калининградской областях, а также в Ингушетии.

Традиционно мошенничество является самым ярким фейковым преступлением, совершаемым путем обмана [3, с. 117]. Цифровые технологии «обновили» мошеннический обман в своей сущности, оставляя за мошенничеством традиционный способ его совершения [4, с. 112], но расширяя схемы обмана [5, с. 32] с помощью цифровой трансформации.

Новая схема мошеннического обмана заключается в следующем. Мошенники звонят от имени сотрудников МФЦ и говорят, что на ваше имя на обозначенный вполне реальный адрес МФЦ пришло письмо, и заодно интересуются, придете ли вы его получать лично или отправить вам его на почту по месту прописки. Независимо от ответа абонента, к примеру, человек просит отправить письмо к нему на почту, звонящий говорит, что сейчас вам в СМС придет номер данного отправления, и его обязательно нужно подиктовать. Во время разговора приходит СМС, только это не номер отправления письма, а обычный код для подтверждения кредита на сайте «Банки. ру». То есть мошенники начинают регистрацию на известном сайте «Банки. ру» по номеру сотового телефона, а СМС им нужен для подтверждения регистрации на сайте. То есть если ввести номер из СМС, то происходит регистрация на сайте «Банки. ру», и кредит берется даже без участия самого потенциального кредитора.

По мнению председателя Забайкальского краевого суда Максима Нестерова, жертвами телефонного мошенничества становятся люди независимо от статуса, занимаемой должности и профессии, поскольку единого портрета жертвы цифрового мошенничества нет. Жертвы заходят в онлайн-банк и переводят деньги мошенникам, при этом жертвами подобных преступлений становились и работники судебного аппарата, и полицейские, и адвокаты, и известные ученые в области уголовного права.

Тенденция нового цифрового мошенничества следующая. Мошенники представляются руководителем той организации, где работает их жертва, создают в Telegram профиль — дубликат профиля руководителя (ректора, директора и т. д.). При этом мошенники тщательно готовятся к «разработке» жертвы, предварительно тщательно изучив ее связи, образ жизни, привычки и даже психологию, а также банки, в которых находятся счета жертвы, и даже суммы на счетах, замотивировав, что они занимаются спецоперацией ФСБ, которая, конечно же, является сверхсекретной и разглашению не подлежит. Такая тенденция идет по всем российским городам. Безусловно, на данном этапе всплывает вопрос о защите персональных данных, хотя бы клиентов банка [6, с. 127]. К нашему сожалению, сегодня в России о такой защите пока не может быть и речи, учитывая многочисленные эпизоды «слития» информации о своих клиентах самими банками.

Полицейские, занимающиеся киберпреступлениями, утверждают, что современным цифровым мошенникам даже не нужна кража персональной личной информации, так как люди сами о себе помещают в соцсетях и на маркетплейсах подробную информацию.

И тем не менее, по нашему глубокому убеждению, противодействие мошенничеству [7, с. 258] в условиях цифровой трансформации возможно только в том случае, если каждому будет обеспечена полная защита персональных данных, которую на данном этапе развития России можно лишь планировать [8, с. 262].

За первую половину 2024 г. россияне отдали мошенникам больше 9 млрд руб. Для сравнения: за 2023 г. кибермошенники похитили у жителей России почти 16 млрд руб., денежные потери растут на данный момент на 11%. Такие данные обсуждались на брифинге в Доме Правительства Республики Татарстан в октябре 2024 г. С января по октябрь в полицию от татарстанцев поступило более 25 тыс. заявлений о преступлениях в сфере информационных технологий, что почти на 45% выше, чем за аналогичный период прошлого года.

Наиболее распространенные виды цифрового мошенничества следующие [9, с. 43].

Одна из самых известных схем мошенников — это звонок от сотрудника службы безопасности банка. Аферисты звонят человеку и сообщают ему о том, что кто-то якобы получил доступ к его счету. Или присылают СМС якобы от банка с различными текстами: «Ваша карта заблокирована», «По вашей карте произведено списание денежных средств» и т. д. После этого жертве звонят и предлагают «спасти сбережения и перевести их на безопасный счет». У жертвы просят пароли от личных кабинетов, а получив их, списывают все доступные средства.

17 сентября 2024 г. в Авиастроительном суде Казани начался уголовный процесс по делу 24-летнего Дмитрия Баранова о мошенничестве в особо крупном размере, совершенном при помощи цифровых технологий.

В конце 2023 г. с 77-летним Юрием Ахрамиевым связался человек, выдавший себя за майора полиции из Казани. Сообщил ему, что его сбережения находятся в опасности, как и его квартира, и предложил продать имущество. Юрий Ахрамиев, поскольку, по собственному признанию, очень доверял сотрудникам правоохранительных органов, согласился. Мошенник помог ему связаться с риелтором и продать квартиру за 3 млн 800 тыс. руб. Несмотря на то что риелтор предупреждала пожилого мужчину о мошенниках, квартиру он все-таки продал. Тогда неизвестный снова связался с Юрием Ахрамиевым и сообщил, что скоро к нему приедет сотрудник с позывным или кодовым словом «цветочек», ему нужно будет передать сумку с деньгами. Дмитрий Баранов как раз и был тем курьером. Вместе со своими сбережениями пенсионер отдал мошенникам около 11 млн руб.

В Казани в сентябре 2024 г. пенсионерка продала квартиру по указанию мошенников и отдала им 7 млн руб. На телефон 77-летней пенсионерки поступил звонок. Звонивший сообщил, что с ее счета якобы были похищены деньги, и, чтобы сохранить накопления, нужно будет следовать указаниям полицейского, который свяжется с ней. Позже ей по видеосвязи позвонил фейковый сотрудник полиции, который сообщил, что неизвестные лица также покушаются и на ее квартиру. Следуя инструкциям по телефону, женщина продала свою квартиру, а вырученные от сделки деньги передала курьеру. Всего она передала мошенникам порядка 7 млн руб.

В Московском суде г. Казани начался процесс по уголовному делу о мошенничестве, где на скамье подсудимых оказалось сразу 16 человек. Им инкриминировали мошенничество в особо крупном размере и участие в преступном сообществе. Девятерых из них обвиняют в незаконном обороте банковских карт. Большинство подсудимых — молодые люди до 30 лет. По версии следствия, группи-

ровка телефонных мошенников действовала по всей России. Их жертвами чаще всего становились беззащитные люди преклонного возраста. Работала банда по известной схеме: представлялись сотрудниками банков, ФСБ, правоохранительных органов и предлагали перевести деньги на безопасный счет. Звонки пенсионерам поступали из-за границы. «Безопасными счетами», на которые предлагалось перевести деньги, были счета карт, их добывали эти 16 человек, которые оказались на скамье подсудимых. По версии следствия, они получали деньги от пенсионеров из Омска, Тюмени, Татарстана, Кировской области, Хабаровска, Амурской области, Москвы и Московской области. Теперь каждому из них грозит как минимум от 5 до 10 лет лишения свободы.

Мошенничества в цифровом поле включают в себя мошенничества под видом предлагаемой диспансеризации.

В одном из мессенджеров 69-летнему казанцу позвонила женщина по имени Светлана, которая представилась работницей медицинского учреждения. Она предложила ему сделать флюорографию в рамках диспансеризации. Во время общения звонившая уговорила мужчину включить демонстрацию экрана своего смартфона. Следуя ее инструкциям, мужчина зашел в банковское приложение, после чего экран его телефона отключился на полчаса. В течение этого времени мошенница оставалась на связи. Когда смартфон снова заработал, мужчина заметил, что с его кредитных карт пропало 330 тыс. руб.

Мошенники также под видом предлагаемой бесплатной сдачи анализов для диспансеризации заставляют жертву продиктовать свой СНИЛС, тем самым получая доступ к его кабинету на Госуслугах.

В современных реалиях также назрела острая необходимость уголовного наказания за использование дипфейков, под которыми понимается изображение, голос или видео, созданное на основе и с использованием искусственного интеллекта, когда нейросеть по пикселям собирает ролик на основе готовых изображений.

Создавая фальшивые аккаунты, мошенник выманивает деньги у граждан под видом известного человека, к примеру, руководителя организации. В Госдуму внесен проект в сентябре 2024 г. о повышенном уголовном наказании за клевету и мошенничество с использованием методики дипфейков, т. е. данная методика будет выступать квалифицирующим признаком названных преступлений.

Более 50% россиян считают дипфейки опасными вследствие распространения дезинформации и, как итог, принятия неверных решений. В интернете содержится масса советов, как отличить искусственный интеллект или контент от реального. Безусловно, стоит обратить внимание на речь человека на видео, его внешний вид, количество пальцев, цвет кожи, повороты головы и движения тела. Тем не менее, независимо от многочисленных подсказок для распознания обмана, дипфейки плотно засели в повседневной жизни людей, не удерживая их риска стать жертвами фейковых преступлений.

Многочисленные исследования в США выявили рост числа мошенничеств, связанных с идентификацией личности, а также обеспокоенность клиентов банка по поводу защиты своих персональных данных.

Согласно опросам около 80% россиян опасаются возможных злоупотреблений технологиями deep fake и краж биометрических данных, а 32% опрошенных лиц выразили сомнение в том, что существующие технологии способны защитить их личность.

Многие опрошенные россияне также полагают, что в рамках развития технологические компании должны сделать приоритетным направлением создание передовых решений для выявления фейков и усиления протоколов безопасности.

По мнению директора Центра цифровой экономики и финансовых инноваций профессора Э. Л. Сидоренко, предложение о дополнении уголовного законодательства квалифицированным составом об использовании дипфейков, является обоснованным, но скорее будет логичнее использовать термин не «дипфейки», а «цифровые технологии» применительно к мошенничеству, дабы не ограничивать только «дипфейками» сферу применения особо квалифицированного вида мошенничества [10, с. 30].

В Ново-Савиновский суд Казани поступило дело курьера кибермошенников. Пожилая жительница Казани рассказала, что мошенникам удалось по телефону подделать голос ее подруги, которую она знает уже больше 60 лет. Женщина, чтобы помочь подруге, отдала курьеру полмиллиона, которые получила от продажи дачи [11, с. 403].

Мы убеждены, что сегодня в России полностью отсутствует защита персональных данных, что непосредственно влияет на изобретение и рождение новых схем мошенничества, фейков, дипфейков в современных условиях цифровых реалий. Мы уверены, что полный пересмотр защиты персональных данных в России, а также противодействие с помощью правовых средств сможет сдержать развитие мошенничества в цифровом поле, а также противодействовать иным фейковым преступлениям [12, с. 390].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бимбинов А. А. Преступления с использованием мобильного банкинга // Уголовный процесс. 2024. № 10 (238). С. 70–75. EDN WTCNYQ.

2. Кабанов П. А. Жертвы киберкраж как объект современной российской кибервиктимологии: криминологический анализ статистических показателей криминальной виктимности 2021–2022 гг. // Виктимология. 2024. Т. 11, № 1. С. 25–42. DOI 10.47475/2411–0590–2024–11–1–25–42. EDN TJLGYE.

3. Малышева Ю. Ю. Мошенничество при получении выплат: актуальные проблемы квалификации / Ю. Ю. Малышева // Право и государство: теория и практика. 2019. № 4. С. 117–118. EDN GVUXNE.

4. Малышева Ю. Ю. Обман как способ совершения мошенничества с использованием электронных средств платежа по зарубежному законодательству // Право и государство: теория и практика. 2019. № 2. С. 111–113. EDN ZSUSPZ.

5. Малышева Ю. Ю. Проблемы квалификации обмана как способа совершения мошенничества с использованием электронных средств платежа // Мониторинг правоприменения. 2018. № 4. С. 31–33. EDN YTVDYL.

6. Малышева Ю. Ю. Обман как способ совершения мошенничества в сфере компьютерной информации // Право и государство: теория и практика. 2018. № 9. С. 126–128. EDN YTAOHR.

7. Малышева Ю. Ю. Обман как основной способ совершения преступлений в условиях COVID-19 // Государство и общество: актуальные вопросы взаимодействия : материалы III Всерос. науч.-практ. конф. с междунар. участием, Казань, 12 марта 2021 г. Казань : ЮрЭксПрактик, 2021. С. 258–260. EDN PVYQMT.

8. Малышева Ю. Ю. О мошенничестве с использованием электронных средств платежа в условиях пандемии COVID-19 // Государство и общество: актуальные вопросы взаимодействия : материалы III Всерос. науч.-практ. конф. с междунар. участием, Казань, 12 марта 2021 г. Казань : ЮрЭксПрактик, 2021. С. 261–263. EDN OTWQIE.

9. Рагулина А. В. Компьютерное мошенничество // Пробелы в российском законодательстве. 2016. № 5. С. 41–49. EDN WDGHIN.

10. Сидоренко Э. Л. Криптовалюта и будущее цифровых финансов. М. : МГИМО МИД России, 2023. 36 с. EDN BZFRJM.

11. Талан М. В. Уголовно-правовая охрана экономических интересов как основа функционирования семьи // Семья и традиционные семейные ценности как духовно-нравственная основа развития общества и государства : сб. материалов Междунар. науч.-практ. конф., Чебоксары, 18–20 апреля 2024 г. Чебоксары : Чувашский государственный университет имени И. Н. Ульянова, 2024. С. 402–408. EDN QMLKVC.

12. Чалышева Ю. В. Фейки: Уголовно-правовая оценка // Закон и общество: история, проблемы, перспективы : материалы XXVII Межвуз. науч.-практ. конф. студентов и аспирантов, Красноярск, 20 апреля 2023 г. Красноярск : Красноярский государственный аграрный университет, 2023. С. 389–391. EDN XNZWBQ.