Для цитирования:
Кисленко С. Л., Фокин А. Д. Мошенничество с использованием информационно-телекоммуникационных технологий как угроза национальной безопасности Российской Федерации // European and Asian Law Review. 2025. № 1. Т. 8. С. 41–54. DOI: 10.34076/27821668_2025_8_1_41.

Information for citation:
Kislenko, S. L. & Fokin, A. D. (2025) Moshennichestvo s ispol`zovaniem informatsionno-telekommunikatsionnykh tekhnologii kak ugroza natsional`noi bezopasnosti Rossiiskoi Federatsii [Fraud Using Information and Telecommunication Technologies as a Threat to the National Security of the Russian Federation]. *European and Asian Law Review*. 8 (1), 41–54. DOI: 10.34076/27821668_2025_8_1_41.

УДК 343.3
BISAC 026000
DOI: 10.34076/27821668_2025_8_1_41.
Научная статья

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

С. Л. Кисленко
Московский государственный юридический университет имени О. Е. Кутафина
ORCID ID: 0009-0003-6751-9034

А. Д. Фокин
Московский государственный юридический университет имени О. Е. Кутафина
ORCID ID: 0009-0002-2943-1464

В настоящее время мошенничество с использованием информационно-телекоммуникационных технологий становится весьма популярным направлением в криминальной среде. В первую очередь это обусловливается привлекательностью для криминала данного направления ввиду наличия потенциальной возможности получения мошенниками сверхприбыли от преступной деятельности. Число преступлений в указанной сфере неуклонно растет. Особенности современной геополитической ситуации, а также масштабность данного вида преступлений обусловливают необходимость рассмотрения последних с позиций обеспечения национальной безопасности Российского государства. Цель исследования – выявить особенности лиц, совершающих мошенничество с использованием информационно-телекоммуникационных технологий с учетом связи их характеристик со способами подготовки, реализации и сокрытия данного вида мошенничества. Отдельная задача – дать криминалистический анализ таким явлениям, как мошеннический call-центр, дропперство. Методологической базой исследования является совокупность различных методологических приемов, средств познания и эмпирического исследования. Применялись и использовались общие и частнонаучные методы познания: формально-логический, системно-структурный, анализ; ситуационный; обобщение и описание;

статистический; сравнение и иные методы. В статье приводятся рекомендации по превенции данного вида преступлений с учетом современного законодательства и правоприменительной практики.

Ключевые слова: *мошенничество, способ преступления, недвижимое имущество, расследование преступлений, call-центр, средства телефонии*

FRAUD USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES AS A THREAT TO THE NATIONAL SECURITY OF THE RUSSIAN FEDERATION

Sergei L. Kislenko
Moscow State Law University named after O. E. Kutafin
ORCID ID: 0009-0003-6751-9034

Andrey D. Fokin
Moscow State Law University named after O. E. Kutafin
ORCID ID: 0009-0002-2943-1464

Currently fraud using information and telecommunication technologies is becoming a very popular area in the criminal environment. First of all, the attractiveness of this area for crime is explained by the potential for fraudsters to receive excess profits from criminal activities. The number of crimes in this area is steadily increasing. The peculiarities of the modern geopolitical situation, as well as the scale of this type of crime are determined, necessitate of the consideration of the latter from the standpoint of ensuring the national security of the Russian state. The purpose of the study is to identify the characteristics of persons who commit fraud using information and telecommunication technologies, taking into account the relationship of their characteristics with the methods of preparation, implementation and concealment of this particular type of fraud. A separate task is to provide a forensic analysis of such phenomena as fraudulent call center, droppery. The methodological basis of the research is a set of various methodological techniques, means of cognition and empirical research. Thus, general and private scientific methods of cognition were applied and used: formal-logical, system-structural, analysis; situational; generalization and description; statistical; comparison and other methods. The article provides recommendations on the prevention of this type of crime, taking into account current legislation and law enforcement practice.

Keywords: *fraud, method of crime, real estate, investigation of crimes, call center, telephony facilities*

Введение

Современные разновидности мошенничества интенсивно интегрируют в цифровую среду. В условиях цифровизации экономического сектора и социума на первый план выходят криминальные способы дистанционного завладения имуществом граждан обманным путем. Среди средств реализации данного вида преступлений значительное место отводится информационно-телекоммуникационным технологиям. Данное обстоятельство предопределило необходимость формирования в рамках стратегии борьбы с преступностью системы эффективных мер противодействия

преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, и снижения ущерба от их совершения (Указ Президента РФ от 7 июня 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»). В эпоху цифровой трансформации мошенничества такие меры направлены на:

1) противодействие использованию преступниками технологии подменных номеров. Современные мошенники активно задействуют IP-телефонию, предоставляющую возможность подключения в упрощенной форме без подтверждения персональных данных абонента[1], используют технологии скрытия данных о местоположении серверов и абонентских устройств (например, путем использования VPN и Proxy-сервисов при совершении вызовов по системе IP-телефонии) и пр.;

2) борьбу с фишингом, используя который злоумышленники пытаются получить конфиденциальную информацию, такую как логины, пароли, номера кредитных карт и другие личные данные, выдавая себя за надежные организации или лиц. В качестве средств реализации современного фишинга мошенники все чаще используют разнообразные интернет-ресурсы (торговые интернет-площадки, социальные сети, онлайн-сервисы и пр.) в целях: сбора информации о потенциальной жертве (интересы, предпочтения и пр.); подготовки мошеннических схем завладения имуществом потерпевшего; распространения фейковой информации и пр. При этом отмечается зависимость данного криминального направления от национальных особенностей. Так, в Бразилии преступники подделывают платформы электронной торговли и телеком-операторов в целях кражи учетных данных; в Китае злоумышленники используют поддельные онлайн-магазины; для России популярным направлением фишинговых атак являются порталы оказания государственных услуг; в ЮАР мошенники рассылают спам-письма с обещанием призов и выигрыша в лотерею[2];

3) противодействие утечкам персональных данных. Продвинутые мошенники могут прибегать к созданию сайтов с объявлениями о продаже товаров, при посещении которых ссылка ведет клиента на фейковую страницу. Здесь либо устанавливаются вредоносные программы для завладения персональными данными банковских карт потерпевших, либо преступники с использованием автоматизированных программ формируют базы данных потенциальных жертв (так называемый парсинг). Парсить могут как торговые площадки, так и социальные сети, онлайн-справочники и прочие базы данных в интернет-пространстве. В последующем такие сведения продаются в Интернете. Так, мошенники call-центров «Milton Group» сумели выкрасть из базы данных крупнейших банков США персональные данные европейских пенсионеров (в частности, информацию о наличии средств на банковских счетах)[3].

Следует также констатировать транснациональный характер большинства видов телефонного мошенничества. В частности, по экспертной оценке специалистов

---

[1] Представляется, что после вступления в силу постановления Правительства РФ от 26 декабря 2024 г. № 1898 «О внесении изменений в некоторые акты Правительства Российской Федерации» совершение мошенничества с использованием IP-телефонии будет затруднительным. Согласно данному документу из перечня лицензий на оказание услуг связи исключается лицензия на передачу интернет-данных с наложением голосовой информации.

[2] Формирование механизма противодействия угрозам информационной безопасности БРИКС – объективная потребность для суверенитета государств-участников межгосударственного объединения // Международная жизнь. URL: https://interaffairs.ru/news/show/45745 (дата обращения: 22.02.2025).

[3] Российских пенсионеров обманывали как немецких // Коммерсантъ. URL: https://www.kommersant.ru/doc/7363194 (дата обращения: 22.02.2025).

Сбербанка, до 90 % call-центров, работающих против граждан РФ, находится на территории Украины. На Россию и все остальные страны приходится не более 10 %[1]. При этом следует отметить, что современное телефонное мошенничество комбинирует коммерческие цели с разведывательными или террористическими. Как отметил Президент России В. В. Путин, против нашего государства развязана масштабная война в киберпространстве[2].

Таким образом, в настоящее время остро стоит вопрос о предотвращении и борьбе с телефонным мошенничеством как с разновидностью угрозы национальной безопасности.

Телефонное мошенничество – международный уровень угрозы

В 2024 г. мошенники похитили у россиян 250–300 млрд руб.[3] При этом все чаще речь идет об организованном и масштабном телефонном мошенничестве, преследующем цели комплексного подрыва стабильности в экономической, социальной и других сферах нашего государства. Мошенники не только похищают денежные средства граждан, но и под предлогом их мнимого возвращения заставляют совершать противоправные (диверсионные, террористические) действия. Так, в декабре 2024 г. ФСБ РФ возбудило уголовное дело о заведомо ложных сообщениях об угрозах террористических актов (ч. 3 ст. 207 УК РФ), направленных на критическую инфраструктуру Москвы, Курска, Брянска и Белгорода. По данным правоохранителей, массовые сообщения и звонки были сделаны по указанию Службы безопасности Украины (СБУ) из call-центров «Milton Group»[4].

При этом аналитики констатируют, что при современном уровне развития преступности ни одна из стран не может самостоятельно организованно и достаточно эффективно бороться с киберпреступлениями[5]. Отсутствие территориальной привязки дистанционного мошенничества, использование современных информационно-телекоммуникационных технологий предполагают консолидацию сил по борьбе с ними на межгосударственном уровне.

В связи с этим страны БРИКС объявили о тесном сотрудничестве для решения этого вопроса. Одним из ключевых аспектов подобного взаимодействия является обмен информацией о киберугрозах и инцидентах. Для этого страны БРИКС активно внедряют механизмы для оперативного информирования друг друга о киберпреступлениях и совместного реагирования на них. Так, по итогам состоявшейся в Москве 10-й встречи рабочей группы объединения по вопросам безопасности в сфере использования информационно-коммуникационных технологий принято решение о формировании реестра контактных пунктов БРИКС для обмена информацией о компьютерных атаках/инцидентах в расширенном составе участников[6].

---

[1] Колл-центр «Бердянск». Телефонные мошенники и схемы обмана // СберБанк: офиц. сайт. URL: http://www.sberbank.ru/ru/person/kibrary/investigations/berdyansk-glava-1 (дата обращения: 22.02.2025).

[2] Путин заявил, что против России развязана война в киберпространстве // ТАСС. URL: https://tass.ru/politika/14686131 (дата обращения: 22.02.2025).

[3] Сбербанк оценил сумму похищенных мошенниками у россиян в 2024 году денег // РБК НОВОСТИ. URL: https://www.rbc.ru/society/11/01/2025/6781f36a9a79478d4e5c2708 (дата обращения: 22.02.2025).

[4] Сообщения о терактах вывели ФСБ на мошеннические колл-центры // Newsinfo. URL: https://www.newsinfo.ru/news/moshennichestvo-koll-centry-fsb/839247/ (дата обращения: 22.02.2025).

[5] Страны БРИКС будут бороться против киберпреступлений сообща // Pravda.ru. URL: https://www.pravda.ru/accidents/1141524-briks/ (дата обращения: 22.02.2025).

[6] БРИКС создаст реестр контактных пунктов для обмена данными о компьютерных атаках // ТАСС. URL: https://tass.ru/politika/20576825 (дата обращения: 22.02.2025).

Важным аспектом сотрудничества выступает также обмен опытом и технологиями в области кибербезопасности. Каждая из стран БРИКС имеет свой уникальный опыт и подход к защите своих киберпространств, и обмен этим опытом позволяет повысить общий уровень кибербезопасности в группе[1].

Пристальное внимание страны БРИКС уделяют проведению совместных действий по борьбе с мошенническими call-центрами. Жертвами массового телефонного мошенничества становятся граждане стран Юго-Восточной Азии, Евросоюза, России. Как констатируют отечественные правоохранительные органы, российские call-центры зачастую являются элементами международной сети мошенников, что затрудняет борьбу с ними силами одного государства. Не так давно ФСБ РФ задержало более десяти руководителей офисов call-центров, которые входили в международную сеть, обманувшую около 100 тыс. человек из более чем 50 стран[2]. В изъятых документах рядом с именами и фамилиями сотрудников call-центров содержалась пометка о языке, на котором они разговаривают (английский, турецкий, казахский и др.). Как свидетельствует практика, работу таких call-центров контролируют международные преступные сообщества.

Проблемы противодействия международным мошенническим call-центрам

К основным проблемам, которые стоят на пути борьбы с международными call-центрами, можно отнести:

различия национального законодательства, в частности отсутствие унификации положений в области информационной безопасности. Это затрудняет создание единых механизмов реализации уголовных и иных мер борьбы с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий;

разный уровень развития стран и разный потенциал в области информационно-коммуникационных технологий;

трудности в установлении всей цепочки мошеннических схем ввиду отсутствия географической привязки деятельности call-центров, их децентрализованности и сетевой структуры, разбросанной по разным государствам, использования Интернета (в том числе сетей разных стран) для осуществления звонков. Так, сеть call-центров «Milton Group» состояла из множества офисов, открытых более чем в 20 странах, которые были укомплектованы штатом сотрудников (операторами, собственной бухгалтерией, охраной, сисадминами);

сложности в отслеживании и идентификации мошенников, поскольку последние используют технологии скрытия данных о местоположении серверов и абонентских устройств, автоматизированной симуляции голоса, а также криптографические транзакции в целях легализации денежных средств, полученных мошенническим путем;

использование преступниками психологических приемов маскировки своих противоправных действий под гражданско-правовые отношения, в связи с чем жертва преступления, не имея реальной возможности распознать истинные намерения мошенников, сама содействует преступникам (например, продавая квартиру

[1] БРИКС и международная безопасность: сотрудничество в борьбе с терроризмом и киберугрозами // TV BRICS. URL: https://tvbrics.com/news/briks-i-mezhdunarodnaya-bezopasnost-sotrudnichestvo-v-borbe-s-terrorizmom-i-kiberugrozami/ (дата обращения: 22.02.2025).

[2] ФСБ пресекла работу международной сети мошеннических call-центров // РБК НОВОСТИ. URL: https://www.rbc.ru/politics/09/12/2024/6756767c9a79473b4e7f280c (дата обращения: 22.02.2025).

либо оформляя кредит под залог недвижимости). Это усложняет раскрытие подобных преступлений;

проблемы, связанные с механизмами: направления правоохранительными органами разных стран друг другу запросов о международной правовой помощи; обмена статистическими данными в сфере борьбы с указанными криминальными явлениями;

отсутствие координационных центров при реализации совместных мероприятий в области борьбы с телефонным мошенничеством, в том числе по линии правоохранительных органов и спецслужб;

отсутствие единого стандарта обмена конфиденциальной информацией, в том числе персональными данными, что приводит к многообразию криминальных способов и технологий их утечки и получения;

слабую разработанность методики расследования транснациональных преступлений.

Мошеннический call-центр как криминальное явление

В целом в настоящее время можно говорить о появлении в практике борьбы с телефонным мошенничеством такой категории, как «мошеннический call-центр». Будучи разновидностью организованной преступной группы, он представляет собой *имеющую признаки организованности устойчивую группу лиц, объединенную в целях получения прибыли посредством совершения массовых мошеннических деяний, направленных на неопределенный круг лиц и совершаемых с использованием информационно-телекоммуникационных технологий*.

Такие центры могут быть классифицированы по: а) структуре (локальные (замкнутые) и имеющие признаки сетевой деятельности); б) целям деятельности (исключительно коммерческие или сопряженные с диверсионными или террористическими); в) географии деятельности (международные и национальные); г) локации (расположенные в зданиях, офисах, промзонах или в местах отбывания наказания (по данным отдельных исследователей, до 60 % всех случаев телефонного мошенничества совершаются из мест лишения свободы) [Бойцов, 2016: 108]); д) штату (крупные (свыше 10 сотрудников в одном офисе), средние (до 10)).

В настоящее время отмечается тенденция совершения телефонного мошенничества одним-двумя преступниками по типу функционирования call-центров. Преступники, как правило, оснащены SIM-боксами, специализированными приложениями, создающими фоновый звук для убедительности (имитация, например, работы офиса), а также базами данных телефонных номеров. Используя такую базу, они могут осуществлять роботизированный «обзвон» или рассылку оповещений (SMS, голосовая почта) потенциальным жертвам. Действия таких мошенников обычно не носят международный характер.

Как показали наши исследования, call-центру присущи следующие устойчивые характеристики:

дистанционный характер деятельности (в том числе транснациональный);

непродолжительность деятельности в пределах одной локации (как правило, не более месяца);

использование современных информационно-телекоммуникационных технологий (как для подготовки, совершения, так и для сокрытия преступления);

тщательное планирование деятельности: моделирование криминального бизнес-процесса; подготовка схем и сценариев обмана; алгоритмизация работы (по-

следовательность звонков, их частота); единые принципы отбора потенциальных жертв; типовые программы и способы обработки жертв;

структурированность организации (единое руководство, наличие лидера и распределение ролей между другими участниками), наличие признаков сетевой деятельности;

анонимность участников (использование кличек и псевдонимов) и многонациональность (для работы в нескольких странах);

ориентация на использование приемов психологического воздействия на жертв;

комбинирование коммерческих целей (скам-схемы, финансовые пирамиды, продажа товаров). Факультативно могут реализовываться и иные противоправные цели (в том числе террористические, диверсионные);

использование средств и приемов конспирации (в частности, путем задействования современных технологий: криптографических средств, IP-телефонии и пр.).

Что касается характеристики call-центров как места реализации телефонного мошенничества, то в качестве таковых, по данным обобщения следственной практики, преступники используют неприметные здания или офисные помещения, а также арендованные квартиры и домовладения. При этом надо учитывать, что локализация таких центров каждый месяц меняется, а при переезде проводится генеральная уборка в офисе, что может затруднить выявление следов. Рабочие места комплектуются столами с компьютером, серверным оборудованием, устройствами агрегации SIM-карт, средствами связи и гарнитурой (наушники и микрофон). Также в помещении может иметься: сейф, счетчики купюр, множительная техника, шредер для уничтожения документов. Сотрудники таких центров могут снабжаться «методической» литературой и инструкциями – так называемыми скриптами. Последние могут дифференцироваться в зависимости от типа клиента, сценария диалога с жертвой и вариантов развития ситуации. В компьютере может размещаться телефонная база клиентов, страницы торговых площадок, информация о потенциальных «клиентах» («лиды»).

Структурированность call-центров предполагает распределение ролей между его участниками.

1. *Руководитель (организатор)*, занимающийся вопросами безопасности деятельности, созданием видимости легальности способов завладения имуществом граждан, отмыванием денежных средств, разработкой и совершенствованием новых способов мошенничества, финансированием (закупка оборудования, пластиковых карт, оформленных на подставных лиц, и пр.). Также эти лица могут заниматься организацией размещения call-центров и их оборудованием. Как правило, такие офисы меняются с периодичностью раз в месяц. Ввиду наличия постоянной необходимости в подборе специфических объектов (неприметные здания или офисы с изолированными входами) такие услуги организатору оказывают постоянно взаимодействующие с ним риелторы, предоставляющие на регулярной основе и помощь в работе с потенциальными жертвами. Данные посредники часто осведомлены о «серых» схемах бизнеса. Среди организаторов телефонного мошенничества высок процент ранее судимых лиц.

2. *Сотрудники кадровой службы и службы безопасности*, осуществляющие подбор и обучение новых сотрудников, а также обеспечение охраны помещений call-центров, руководящего звена и внутреннюю безопасность. Сотрудники набираются в основном из числа студентов, которые обладают коммуникативными навыками, а также навыками работы с информационно-телекоммуникационными технологиями. Так, в ликвидированных call-центрах «Milton Group» в 2023 г. трудились сотни

операторов, которых привлекали из иностранных вузов. Они отвечали за определенный регион в зависимости от знания языка[1].

3. *Информаторы и консультанты*, предоставляющие преступникам необходимую информацию о потенциальных жертвах и принадлежащем им имуществе (сотрудники социальных служб, МФЦ, Росреестра и пр.) либо оказывающие «консультативную» помощь в создании преступных схем, а также разного рода «методических» рекомендаций (бывшие сотрудники банков, финансовых организаций, знакомые с моделями поведения клиентов, психологи и пр.). Если цели функционирования call-центра, наряду с коммерческой, имеют террористическую, диверсионную направленность, то такие центры курируются сотрудниками спецслужб. Последние снабжают работников call-центров методической литературой, содержащей современные технологии манипулирования и зомбирования людей в целях совершения ими терактов или диверсий (поджогов военкоматов, зданий администрации и пр.) под предлогом возвращения полученных от них обманным путем денежных средств. По мнению специалистов НКЦКИ[2], функционирование большинства call-центров, действия которых направлены против граждан России, было четко скоординировано из других стран.

4. *Операторы*. Данные лица по степени криминальной квалификации могут подразделяться на две категории: неквалифицированные, осуществляющие звонки в целях установления контакта с жертвой, выяснения сведений о его имущественном положении; квалифицированные менеджеры, использующие профессиональные приемы психологической манипуляции (выдающие себя за сотрудников банков, правоохранительных органов и пр.). Коммуникативная сторона способов реализации обмана или злоупотребления доверием связана с уловками преступников, направленными на инициирование совершения жертвой разнообразных операций с имуществом (движимым и недвижимым). Ключевое место в анализируемых криминальных деяниях отводится методам социальной инженерии. Последние в симбиозе с телекоммуникационной составляющей образуют такой способ телефонного мошенничества, как «Вишинг». Последний, являясь одним из видов фишинга, заключается в том, что злоумышленники, используя телефонную или интернет-коммуникацию и играя определенную роль (сотрудника банка, правоохранительных органов, покупателя недвижимости и т. д.), создают ситуацию, позволяющую манипулировать человеческими чувствами, и под разными предлогами выманивают у жертвы конфиденциальную информацию или стимулируют на совершение заранее запрограммированных преступником действий со счетами (денежными средствами) или принадлежащим жертве имуществом [Меньщиков, Федосенко, 2021: 38].

5. *Технический персонал*, отвечающий за: а) функционирование средств телефонии (например, создание анонимайзеров для интернет-соединений при совершении вызовов по системе IP-телефонии; поиск баз данных клиентов; обеспечение операторов «белыми» номерами и пр.); б) мониторинг торговых интернет-площадок («Авито», «Юла» и пр.), социальных сетей и пр.; в) размещение «объявлений-ловушек», содержащих вымышленную информацию о продаваемом товаре и о продавце и пр. (в целях введения покупателя в заблуждение, привлечения его внимания красивыми фотографиями, невысокой ценой товара, чтобы получить номер телефона); г) создание электронных кошельков («QIWI», «Яндекс-кошелек»,

[1] Российских пенсионеров обманывали как немецких.

[2] Национальный координационный центр по компьютерным инцидентам Федеральной службы безопасности России.

«Webmany» и др.); д) создание и использование специализированных компьютерных программ, направленных на автоматизированный сбор сведений о потенциальных жертвах: истории покупок, место работы, имена близких (например, путем использования Telegram-ботов) и пр.

6. *Лица, привлекаемые или используемые мошенниками для оказания валютно-финансовых услуг, в том числе в сфере легализации преступного дохода*. В условиях цифровизации современной экономики в качестве таких посредников зачастую выступают:

лица, имеющие аккаунты в криптовалютных системах. Денежные средства, полученные мошенниками, могут составлять значительные суммы (ч. 4 ст. 159 УК РФ). При дальнейшем их размещении в криптовалюте это объективно предполагает задействование достаточного количества таких аккаунтов (и посредников), поскольку последние имеют определенные ограничения на максимально допустимую сумму, при которой не нужна идентификация личности. По данным Банка России, наиболее популярным способом купли-продажи криптовалюты в преступной среде является использование теневых обменных сервисов, работающих в анонимных сетях (Darknet)[1]. При этом преступники чаще всего прибегают к использованию криптокошельков. Объясняется это в первую очередь относительной доступностью процесса создания криптокошелька без помощи сторонних организаций (например, криптобирж). И самое главное: использование данной схемы позволяет скрыть информацию о совершаемых транзакциях. В частности, мошенники часто переводят криптовалюту (например, Bitcoin) между множеством криптокошельков, постоянно изменяя суммы переводов. Однако даже при такой усложненной схеме транзакции всех пользователей записываются в общедоступной базе данных (блокчейне) и становятся доступными для отслеживания. Поэтому более продвинутые преступники могут пользоваться специализированными сервисами, позволяющими за комиссию от переведенных, например, Bitcoin получить другие счета в криптовалюте, которые никак не будут связаны с мошенником («Тумблеры»), или предлагающими смешивание криптовалюты множества участников с последующим ее отправлением по разным кошелькам («Миксеры») [Гусева, 2018: 39];

лица, которые за небольшой процент предоставляют счета своих банковских карт для обналичивания или перевода денег. Следует констатировать, что за последнее десятилетие в области совершения дистанционного мошенничества сложилось устойчивое криминальное явление – *дропперство*. Оно представляет собой процесс вывода денег со счетов преступников в целях их легализации посредством использования банковских карт подставных лиц. Механизм дропперства следует рассматривать в рамках теории преодоления противодействия расследованию. В частности, данный механизм используется мошенниками для сокрытия следов криминальных действий и создания затруднений у правоохранительных органов в установлении причинно-следственных связей между реквизитами, используемыми мошенниками, и их преступными действиями. Дропперы могут подразделяться по степени их информированности о преступных действиях мошенников на осведомленных и нет[2]. Чаще всего в качестве представителей последней категории выступают подростки, пенсионеры и мигранты, которых мошенники заманивают

[1] Криптовалюты: тренды, риски, меры: доклад для общественных консультаций. URL: https://cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf (дата обращения: 22.02.2025).

[2] За первый квартал 2024 г. число банковских операций без согласия клиента составило 300 тыс., а ущерб – 4,3 млрд руб. Представляется, что значительную часть таких операций было бы практически невозможно осуществить без участия дропов. См.: Дропперы без страха, но с упреком // Коммерсантъ. URL: https://www.kommersant.ru/doc/6789047 (дата обращения: 22.02.2025).

в такую схему обманным путем под предлогом получения легкого заработка (например, вербовка посредством размещения объявлений о вакансиях сотрудников разных «выгодных» инвестиционных проектов). Так, только с конца 2023 г. нотариусы передали в Росфинмониторинг более 2 тыс. сообщений о «подозрительных» доверенностях на открытие банковских счетов. Эти данные помогли правоохранителям выявить лиц, которые дают доступ к своим счетам мошенникам для кражи и отмывания денег[1].

Заключение

Подводя итог, хотелось бы отметить, что повышенная латентность телефонного мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий, обусловлена отчасти трансформацией современного информационного общества, которое не имеет ярко выраженных социальных, экономических, технологических границ. В связи с этим развитие современных методов борьбы с данными преступлениями предполагает решение ряда следующих задач.

1. Создание системы международной информационной безопасности, предусматривающей совокупность международных и национальных институтов, регулирующих деятельность в глобальном информационном пространстве в целях предотвращения (и минимизации) угроз международной информационной безопасности[2]. Это предполагает создание многосторонних соглашений в области борьбы с международной преступностью (например, по возврату из-за рубежа доходов, полученных преступным путем).

2. Повышение цифровой грамотности населения России и других стран. Борьба с телефонным мошенничеством должна идти и в просветительском поле. Стоит констатировать, что этому направлению государство уделяет недостаточное внимание. В большинстве своем законодатель акцентирует внимание на запретах в отношении инструментов телефонного мошенничества. Так, в настоящее время объектами рекламы не могут быть как сама цифровая валюта, так и услуги криптообменников или криптокошельков (Федеральный закон от 8 августа 2024 г. № 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»). При всей прогрессивности данных шагов, на наш взгляд, они должны реализовываться в комплексе с иными мерами информационной борьбы. В частности, необходимо регулярное освещение этой темы в СМИ в виде программ, интервью с должностными лицами, публикаций, видеосюжетов, социальной рекламы по вопросам профилактики и противодействия современным мошенническим схемам. Также представляется целесообразным внедрение в повседневную жизнь граждан цифровых приложений – памяток, в которых будет собрана информация о наиболее распространенных схемах мошенничества. Так, Министерство цифрового развития, связи и массовых коммуникаций РФ планирует разработать приложение, где будет предусмотрена тревожная «красная кнопка» для оперативного взаимодействия с разными ведомствами и участниками рынка. Если человеку поступит телефонный вызов от мошенников, он сможет быстро уведомить об этом банки и операторов связи[3].

---

[1] Финразведка стала активнее следить за доверенностями на банковские счета // РБК НОВОСТИ. URL: https://www.rbc.ru/finances/02/05/2024/662d18af9a7947318834c1e8 (дата обращения: 22.02.2025).

[2] Такой подход всецело вытекает из Основ государственной политики Российской Федерации в области международной информационной безопасности. См.: Указ Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СПС «Гарант». URL: https://www.garant.ru/products/ipo/prime/doc/400473497/ (дата обращения: 22.02.2025).

[3] Борьба с телефонным мошенничеством // Tadviser. URL: https://www.tadviser.ru/index.php/Статья:Борьба_с_телефонным_мошенничеством (дата обращения: 22.02.2025).

3. Формирование на уровне государств единых центров противодействия мошенничеству, объединяющего работу правоохранительных органов, банков, крупных операторов связи и владельцев интернет-ресурсов в целях оперативного обмена базами данных о фактах выявленных мошеннических действий и лиц, их совершивших. На наш взгляд, перспективным направлением видится развитие идеи создания отдельных антимошеннических call-центров, в задачи которых будет входить нейтрализация мошеннических call-центров. Положительной тенденцией в данном направлении видится внедрение сервиса «Фрод-рулетка», позволяющего в режиме реального времени перехватывать звонки мошенников и перенаправлять их на специально подготовленных пользователей. Это не только помогает выявлять актуальные схемы мошенников, но и нейтрализует их, так как они не могут в это время связаться с реальной жертвой. Так, с помощью данной платформы был выявлен новый сценарий мошенников с «Почтой России», который ранее не использовался в таком виде[1].

4. Внедрение передовых технологий и автоматизация технологической стороны банковских операций путем разработки платформ, способных выделять из потоков финансовой информации подозрительные операции и блокировать их, а также создание баз данных о случаях и попытках осуществления переводов денежных средств без согласия клиентов. Например, Роскомнадзор в целях усиления борьбы с телефонным мошенничеством в декабре 2022 г. запустил единую платформу верификации телефонных вызовов (ЕПВВ) «Антифрод», предназначенную для упрощения процесса получения данных об их подлинности и блокировки звонков и сообщений с подменных номеров. Положительно зарекомендовала себя и платформа «Антифишинг» по блокировке вредоносных интернет-страниц. В результате по итогам второго квартала 2024 г. количество операций, проведенных без добровольного согласия клиентов, заметно сократилось[2]. Немалое значение имеет обмен опытом, технологиями и наработками в сфере борьбы с мошенничеством между банковскими структурами разных государств. Так, Сбербанк поделится своим опытом в сфере обеспечения кибербезопасности и противодействия мошенничеству со странами БРИКС (на примере внедренной антифрод-платформы)[3].

5. Реализация законодателем мер по более жесткой регламентации оборота SIM-карт без предъявления паспорта и установления личности покупателя (в частности, усиление ответственности за заключение от имени оператора связи договора с абонентом, данные которого либо не указаны, либо оформлены на подставное лицо); SIM-боксов для оказания услуг мобильной связи (например, только при наличии договора с оператором связи). Данные шаги имеют существенное значение в превенции анализируемого вида криминальных деяний (особенно в направлении борьбы с call-центрами).

6. Ужесточение на уровне уголовной политики современного Российского государства ответственности в отношении лиц, которые умышленно предоставляют свои банковские карты в целях хищения денежных средств у граждан (дропперов). Поскольку подобные деяния совершаются в большинстве своем в составе организованной группы, их следует относить к категории тяжких преступлений. Представ-

[1] «Фрод-рулетка» начала менять сценарий с мошенниками – хищник сам становится добычей // Известия. URL: https://iz.ru/1730678/natalia-revva/frod-ruletka-nachala-meniat-stcenarii-s-moshennikami-khishchnik-sam-stanovitsia-dobychei (дата обращения: 22.02.2025).

[2] Против телефонных мошенников будут внедрены сразу тридцать технологических мер // RGRU. URL: https://rg.ru/2024/11/25/na-korotkom-provodke.html (дата обращения: 22.02.2025).

[3] Сбер поможет странам БРИКС улучшить кибербезопасность // Газета.ru. URL: https://www.gazeta.ru/business/news/2024/04/27/22887019.shtml (дата обращения: 22.02.2025).

ляется, что такая ответственность должна распространяться и на иных лиц, оказывающих содействие мошенникам. В данном аспекте интересен опыт Китая, где усиление борьбы с мошенничеством в сфере телекоммуникаций связано с введением мер и ограничений в отношении лиц, которые продают или предоставляют в аренду преступникам свои аккаунты, SIM-карты, порты для SMS, цифровые кошельки, а также помогают мошенникам выполнять аутентификацию по реальному имени для таких инструментов и пр. Данные лица и организации, помимо наказания, будут внесены в список недобросовестных, информация о них будет загружена на национальную платформу для обмена кредитной информацией в целях оперативной передачи таких сведений другим органам. Указанным людям и организациям устанавливается запрет на открытие новых счетов для онлайн-платежей, а также ограничивается функционал телекоммуникационных средств на их имя (включая стационарные телефоны, SIM-карты, веб-сайты и пр.)[1]. Также требует ужесточения ответственность за умышленную массовую утечку персональных данных (номера банковских карт, телефонов, фамилий граждан). Представляется, что в современных условиях такие преступления нужно рассматривать с позиций обеспечения национальной безопасности страны. Это закономерно требует унификации массива нормативных правовых актов, регулирующих обработку персональных данных, а с позиций международного сотрудничества в области борьбы с преступностью – детализации законодательства по защите персональных данных в части регулирования передачи данных между странами БРИКС[2].

7. Введение на законодательном уровне обязанности владельцев сервисов размещения объявлений и имущественных агрегаторов товаров и услуг (таких как «Циан», «Авито» и пр.), имеющих обширную аудиторию пользователей и содержащих платежную информацию, проводить идентификацию через единую систему идентификации и аутентификации (ЕСИА) тех продавцов, кто намерен разместить объявление о продаже товаров или услуг.

8. Реализация сбалансированного (в рамках уголовной и экономической политики) подхода в процессе интеграции цифровой валюты в современную экономику. С одной стороны, должна быть обеспечена централизованная система мониторинга за оборотом криптовалюты в Российском государстве в целях повышения эффективности мер по борьбе с незаконными операциями с такой валютой (в частности, с легализацией доходов). Так, в России для борьбы с преступлениями в сфере криминального оборота криптовалюты начали активно внедрять специальное программное обеспечение, которое используется как для финансового мониторинга, так и для расследования уголовных дел[3]. С другой стороны, ввиду роста популярности цифровой валюты у преступников нужно не допустить потерю доверия к ней добросовестных участников рынка (как следствие, избежать обесценивания криптовалюты, оттока капитала из России, стагнации рынка)[4].

---

[1] В Китае ужесточают меры по борьбе с кибермошенничеством // BRICScompetition. URL: https://bricscompetition.org/ru/news/measures-to-be-tougher-on-cyberfraud-in-china (дата обращения: 22.02.2025).

[2] В частности, в рамках XV Международного IT-форума в Ханты-Мансийске страны БРИКС выступили с инициативой создания единого стандарта обмена конфиденциальной информацией (в том числе персональными данными). См.: Страны БРИКС планируют разработать единый стандарт обмена персональной информацией // ТАСС. URL: https://tass.ru/obschestvo/21133099 (дата обращения: 22.02.2025).

[3] Страны БРИКС обменялись опытом цифровизации в борьбе с киберпреступностью // Ведомости. URL: https://www.vedomosti.ru/politics/articles/2024/06/20/1044966-strani-briks-obmenyalis-opitom-tsifrovizatsii-v-borbe-s-kiberprestupnostyu (дата обращения: 22.02.2025).

[4] При всей прогрессивности Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты

9. Повышение эффективности реализации механизмов взаимодействия и обмена данными между правоохранительными органами и банками[1], а также иными структурами и организациями. Такое взаимодействие немыслимо без принятия мер, направленных на сокращение сроков исполнения запросов правоохранительных органов (в адрес кредитных организаций, операторов сотовой связи и др.). Немалое значение в данном направлении занимает повышение оперативного доступа и использования следователями цифровой информации, содержащей сведения, имеющие значение для дела и хранящиеся в цифровых базах соответствующих организаций. В этом плане мы поддерживаем мнение А. И. Бастрыкина о том, что лицо, производящее расследование, должно иметь оперативный доступ к базам данных и интернет-ресурсам Центрального банка России, Федеральной нотариальной палаты и пр. [Бастрыкин, 2021: 16].

10. Разработка и усовершенствование криминалистических рекомендаций по расследованию данного вида преступлений с учетом их видовых особенностей. Как уже отмечалось, значительная часть анализируемых преступных посягательств носит транснациональный характер, что существенно затрудняет деятельность правоохранительных органов разных стран в рамках информационного, ведомственного, юрисдикционного, технического, методического взаимодействия. Это закономерно требует формирования криминалистических методик расследования транснациональных преступлений.

11. Совершенствование и дальнейшая автоматизация процесса сбора, систематизации, обработки и анализа сведений о дистанционных преступлениях, совершенных с использованием информационно-телекоммуникационных технологий (на примере российской системы «Дистанционное мошенничество» (введена приказом ГУ МВД России по г. Москве от 5 апреля 2021 г. № 121)).

Библиографический список

Бастрыкин А. И. Цифровые технологии современной криминалистики // Вестник Академии Следственного комитета РФ. – 2021. – № 2. – С. 11–17.

Бойцов Ю. М. Проблемы проверки, выявления и раскрытия мошенничества с использованием мобильных средств связи // Вестник Санкт-Петербургского университета МВД. – 2016. – № 2. – С. 107–112.

Гусева А. А. Возможные пути решения проблемы легализации денежных средств через криптовалюту // Экономика. Право. Инновации. – 2018. – № 5. – С. 36–45.

Меньщиков А. А., Федосенко М. Ю. Возможности применения методов социальной инженерии в организации телефонного мошенничества // Экономика и качество системы связи. – 2021. – № 4. – С. 36–47.

Российской Федерации», которым закреплен запрет на использование криптовалют как платежного инструмента для резидентов РФ, следует отметить, что ограничение использования данной валюты в процессе расчета за товары, работу и услуги, является фактором, не только сдерживающим развитие отечественных платежных систем и онлайн-сервисов, но и стимулирующим поиск криминалом новых обходных путей.

[1] В частности, с 2023 г. сотрудники МВД РФ могут оперативно получать данные об операциях без согласия клиента из автоматизированной системы ФинЦЕРТ (Центр взаимодействия и реагирования Департамента информационной безопасности) Банка России. Информацию, полученную от правоохранительных органов, банки смогут учитывать для предотвращения новых мошеннических операций (Федеральный закон от 20 октября 2022 г. № 408-ФЗ «О внесении изменений в статью 26 Федерального закона „О банках и банковской деятельности“ и статью 27 Федерального закона „О национальной платежной системе“»).

References

Bastrykin, A. I. (2021) Tsifrovye tekhnologii sovremennoi kriminalistiki [Digital technologies of modern criminology]. *Vestnik Akademii Sledstvennogo komiteta RF*, (2), 11–17.

Boytsov, Yu. M. (2016) Problemy proverki, vyyavleniya i raskrytiya moshennichestva s ispol`zovaniem mobil`nykh sredstv svyazi [Problems of verification, detection and disclosure of fraud using mobile communications]. *Vestnik Sankt-Peterburgskogo universiteta MVD*, (2), 107–112.

Guseva, A. A. (2018) Vozmozhnye puti resheniya problemy legalizatsii denezhnykh sredstv cherez kriptovalyutu [Possible ways to solve the problem of money legalization through cryptocurrency]. *Ekonomika. Pravo. Innovatsii*, (5), 36–45.

Menshchikov, A. A. & Fedosenko, M. Yu. (2021) Vozmozhnosti primeneniya metodov sotsial`noi inzhenerii v organizatsii telefonnogo moshennichestva [The possibilities of using social engineering methods in the organization of telephone fraud]. *Ekonomika i kachestvo sistemy svyazi*, (4), 36–47.

Информация об авторах

Сергей Леонидович Кисленко – профессор кафедры криминалистики Московского государственного юридического университета имени О. Е. Кутафина, доктор юридических наук, профессор (e-mail: ser-kislenko@yandex.ru)

Андрей Денисович Фокин – ассистент кафедры криминалистики Московского государственного юридического университета имени О. Е. Кутафина (e-mail: raif1136@yandex.ru).

Information about the authors

Sergei L. Kislenko – Professor of the Department of Criminology of the Moscow State Law University named after O. E. Kutafin, Doctor of Juridical Sciences, Professor (e-mail: ser-kislenko@yandex.ru).

Andrey D. Fokin – Assistant Professor of the Department of Criminology of the Moscow State Law University named after O. E. Kutafin (e-mail: raif1136@yandex.ru).

Дата поступления в редакцию / Received: 20.03.2025
Дата принятия решения об опубликовании / Accepted: 15.04.2025