Научная статья
УДК 343.72
doi: 10.33463/2687-1238.2024.32(1-4).2.247-257

АНАЛИЗ ФАКТОРОВ, СПОСОБСТВУЮЩИХ РОСТУ МОБИЛЬНОГО МОШЕННИЧЕСТВА В РОССИИ

Виталий Викторович Копылов[1], Олег Михайлович Прокофьев[2], Алексей Александрович Субботин[3], Артем Анатольевич Истомин[4]
[1, 2, 3] Тверской филиал Московского университета МВД России имени В. Я. Кикотя, г. Тверь, Россия
[1] kopylov_70@inbox.ru
[2] bimtim22@yandex.ru
[3] lexa-subbota@yandex.ru
[4] Псковский филиал Университета ФСИН России, г. Псков, Россия, aristom@mail.ru

Аннотация. В статье исследуются проблемы борьбы с мобильным мошенничеством в России. Анализируются статистические данные, характеризующие развитие мобильного мошенничества в нашей стране. Изучаются особенности мобильного мошенничества, его сильные стороны, в том числе такой прием, как социальная инженерия. Рассматривается разновидность мобильного («тюремного») мошенничества.

Ключевые слова: мобильное мошенничество, социальная инженерия, «тюремное» мобильное мошенничество, киберпреступления, сотрудники правоохранительных органов, противодействие киберпреступлениям

Для цитирования
Копылов В. В., Прокофьев О. М., Субботин А. А., Истомин А. А. Анализ факторов, способствующих росту мобильного мошенничества в России // Человек: преступление и наказание. 2024. Т. 32(1–4), № 2. С. 247–257. DOI: 10.33463/2687-1238.2024.32(1-4).2.247-257.

Человек: преступление и наказание. 2024. Т. 32(1–4), № 2. ISSN 1999-9917 (print). ISSN 2687-1238 (online)
Man: crime and punishment, 2024, vol. 32(1–4), iss. 2, ISSN 1999-9917 (print), ISSN 2687-1238 (online)

Original article

ANALYSIS OF THE FACTORS CONTRIBUTING TO THE GROWTH OF MOBILE FRAUD IN RUSSIA

Vitaly Viktorovich Kopylov[1], Oleg Mikhailovich Prokofiev[2], Alexey Alexandrovich Subbotin[3], Artyom Anatolyevich Istomin[4]
[1, 2, 3] Tver branch of the Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot, Tver, Russia
[1] kopylov_70@inbox.ru
[2] bimtim22@yandex.ru
[3] lexa-subbota@yandex.ru
[4] Pskov Branch of the Federal Penitentiary Service of Russia University, Pskov, Russia, aristom@mail.ru

Аннотация. The article examines the problems of combating mobile fraud in Russia. The statistical data characterizing the development of mobile fraud in our country are analyzed. The features of mobile fraud and its strengths, including such a technique as social engineering, are being studied. A type of mobile fraud is considered – "prison" mobile fraud.

Ключевые слова: mobile fraud, social engineering, "prison" mobile fraud, cybercrime, law enforcement officers, countering cybercrime

Для цитирования
Kopylov V. V., Prokofiev O. M., Subbotin A. A. & Istomin A. A. 2024, 'Analysis of the factors contributing to the growth of mobile fraud in Russia', *Man: crime and punishment,* vol. 32(1–4), iss. 2, pp. 247–257, doi: 10.33463/2687-1238.2024.32(1-4).2.247-257.

Число киберпреступлений в России год от года продолжает неуклонно расти. Так, за 6 лет их количество увеличилось в 10 раз, причиненный ущерб от данных преступлений, по разным оценкам, составляет до 600 млрд руб. в год [2]. Киберпреступность в нашей стране стала реальной угрозой национальной безопасности [1]. В 2022 г. в России было совершено 522,1 тыс. преступлений с использованием IT-технологий, из которых 94 % – телефонное (мобильное) мошенничество. В результате их совершения у граждан было похищено 14,2 млрд руб. (рост суммы украденных денежных средств по сравнению с уровнем прошлого года составил 39 %). Под влиянием телефонных преступников в этом же году российские граждане пытались оформить кредиты на 200 млрд руб., а 83 % граждан России хотя бы раз подвергались попытками кибермошенничества [1]. В целом количество подобного рода мошенничества за 5 лет увеличилось в 2 раза.

Проблеме противодействия киберпреступлениям руководством страны уделяется большое внимание. Так, Президент Российской Федерации В. В. Путин в части совершенствования борьбы с мобильным мошенничеством отметил следующее: «Важно своевременно информировать людей о способах защиты от мошенников, повышать профессиональную подготовку и техническое оснащение органов внутренних дел и не-

обходимо наладить четкое взаимодействие с банковским сообществом, интернет-провайдерами, операторами сотовой связи».

Отличительными чертами мобильного мошенничества являются высокая организованность (четкое распределение ролей среди участников организованных преступных групп (ОПГ), специализация: звонари, дропы, курьеры и т. п.), мобильность при перемещении, конспирация (бесконтактные формы передачи денег, банковских карт и т. п.), знания и практические навыки в сфере IT-технологий, использование возможностей интернет-банкинга, высокотехнологичного оборудования, технологий, позволяющих изменять номера сотовых телефонов, голоса абонентов, различных способов обмана граждан, основанных на психологических особенностях человека, нейролингвистического программирования.

С 2022 г. мошенники в основном совершают звонки из-за пределов России. Это Украина, Казахстан и другие соседние государства. В настоящее время более 90 % мошеннических звонков совершается с территории Украины. В случае задержания злоумышленники, как правило, уже вывели украденные денежные средства со счетов и удалили все имеющиеся электронные следы с аппаратуры. При совершении мобильного мошенничества преступники используют безналичные формы расчетов, деньги, полученные от потерпевших, переводятся на QIWI-кошелек или криптовалюту Bitcoin, а также через интернет-магазин покупают дорогостоящую электронную аппаратуру. Все это позволяет телефонному (мобильному) мошенничеству оставаться самым динамично развивающимся видом кибермошенничества в России (рост числа подобных преступлений составляет около 40 % в год, а их раскрываемость достаточно низкая – 19,3–25 %).

С учетом масштабов и негативных последствий рассматриваемого явления возникает острая необходимость в анализе факторов, которые на протяжении 19 лет способствовали тому, что мобильное мошенничество в нашей стране стало угрозой национальной безопасности.

1. Высокая организация мобильного мошенничества

На наш взгляд, отличительной чертой данного преступления является его высокая организация. Типовая схема организации преступного call-центра включает в себя следующие категории участников: организатор, куратор, звонари, дропы, курьеры[1]. Для размещения преступного call-центра снимается квартира или небольшой офис. Общение внутри ОПГ – только посредством голосовых и SMS-сообщений в мессенджерах WhatsApp, Telegram, личное (визуальное) общение исключено. Руководит ОПГ организатор – человек, который находится на территории соседних государств (Украина, Казахстан) и осуществляет общее, стратегическое руководство call-центром. Обычно под руководством организатора находится несколько call-центров. Следующим участником из числа руководителей является куратор – человек, который находится непосредственно на месте call-центра и фактически организует его деятельность, набирает штат и распределяет обязанности членов ОПГ.

Кроме руководства, имеются исполнители – звонари – лица, которые непосредственно осуществляют общение с гражданами по сотовым телефонам. Они являются основным звеном call-центра и при помощи вербального манипулирования вводят в заблуждение абонентов (граждан), в результате чего получают конфиденциальную информацию относительно банковских карт, убеждают потерпевших совершать раз-

[1] Названия взяты из материалов уголовного дела по факту мобильного мошенничества.

личные манипуляции с денежными средствами. Полученная информация реализуется сразу. Денежные средства со счета законного владельца переводятся на счета электронных кошельков Qiwi, Яндекс либо через интернет-обменники в биткоины. Кроме того, звонари имеют в своем распоряжении технические средства и сервисы для работы мошеннической анонимной телефонии посредством IP-телефонии (Narayana, Black Wolf), благодаря чему они могут менять свой абонентский номер для осуществления исходящих звонков потерпевшему. В результате этого звонари могут представляться сотрудниками правоохранительных органов (ФСБ, Следственного комитета, прокуратуры, МВД) или банка, озвучивая при этом сведения реально действующих сотрудников с настоящего номера служебного телефона [1]. В настоящий момент выявлено и зафиксировано более 500 тыс. номеров сотовых телефонов, которые были использованы в мошеннических схемах. После того как деньги у потерпевшего были забраны (перечислены), подключаются дропы [1]. Дроп – это лицо, обеспечивающее обналичивание полученных у жертвы денег. По разным оценкам, количество дропов в нашей стране достигает 500 тыс. чел. [4]. Они оформляют на себя банковские карты, их количество может достигать несколько десятков штук, либо покупают их у других лиц. На счета банковских карт, подконтрольных дропам, и переводят похищенные у граждан денежные средства. В первом полугодии 2022 г. Сбербанком был заблокирован выпуск 50 тыс. банковских карт, которые могли быть использованы дропами для осуществления мошеннических переводов (АППГ – 17 тыс.) [4]. Дроп при необходимости делает закладку или вносит деньги через другие терминалы на другой банковский счет либо счет электронного кошелька. Есть также своя служба доставки – курьеры. Получив сведения о закладке, курьер забирает ее и доставляет адресату. При этом в обязательном порядке изменяет свой внешний вид, гримируется, делает все, чтобы быть неприметным [1]. Схема управления максимально эффективная, она обеспечивает четкое управление процессом (мобильным мошенничеством) и безопасность руководителей ОПГ. Почти всегда они остаются недосягаемыми для правоохранительных органов, в большинстве своем удается задерживать курьеров, на которых обычно цепочка обрывается.

В настоящее время наиболее актуальным способом совершения телефонных мошенничеств стало использование таких мессенджеров, как: WhatsApp, Viber и Telegram, через которые осуществляется рассылка различного рода сообщений и обращений: «Просьба проголосовать “За”», «Подтвердите актуальность телефонного номера», «Ваш родственник попал в беду», «Подтвердите код из SMS», «Займите небольшую сумму денег» и т. п.

В целом по России в 2022 г. количество мошеннических операций по переводу денежных средств, совершенных с использованием методов «социальной инженерии», увеличилось на 38,8 % (1035,01 тыс.; АППГ – 773,27тыс.), ущерб составил 13 582,23 млн руб. Его основа заключается в том, что в телефонном разговоре с потерпевшими злоумышленники используют различные способы нейролингвистического программирования. Это вызывает личностно-волевые и эмоциональные нарушения и как следствие неспособность человека к адекватной оценке происходящего, то есть у жертвы создается неадекватная оценка цели и смысла совершаемых действий или искаженное представление о цели совершаемых действий. Если раньше результатом мошенничества была только определенная (достаточно небольшая) сумма денег, то сейчас преступники «работают по полной». Пользуясь тем, что потерпевшие, находясь в ситуации,

которую психологи-эксперты описывают как «порок воли»[1] со всеми его составляющими (отсутствие возможности осознавать фактический характер своих действий, неспособность понимать значение совершаемых действий), убеждают жертву продавать свою недвижимость, машины, оформлять на себя кредиты и отдавать все средства злоумышленникам. В результате в мобильном мошенничестве произошел качественный скачок в сторону увеличения размера похищаемой суммы, именно в этом направлении сейчас наблюдается рост числа фактов совершения мобильного мошенничества в особо крупном размере. Так, в Тверской области за 10 месяцев 2023 г. было совершено 181 телефонное мошенничество (АППГ – 92), из них 87 преступлений в особо крупном размере (АППГ – 49).

Необходимо отметить, что более 12 лет действует и успешно развивается в исправительных учреждениях уголовно-исполнительной системы (УИС) специализированная разновидность мобильного мошенничества – «тюремное» мобильное мошенничество. Оно осуществляется заключенными, находящимися в исправительных учреждениях, с помощью сотовых телефонов и соответствующей аппаратуры. С 2011 г. заключенные стали создавать «тюремные» call-центры, которые организованы по типовой схеме, как и «на воле», только некоторые участники ОПГ находятся вне исправительного учреждения и забирают денежные средства у потерпевших. По статистике, один «тюремный» call-центр в среднем за неделю совершает около 20 тыс. звонков потенциальным жертвам, доход от мошеннической деятельности составляет 75 млн руб. в месяц.

По мнению зампреда правления Сбербанка Станислава Кузнецова, 40–50 % мошеннических call-центров находится в исправительных учреждениях, в каждом третьем учреждении есть преступный call-центр. Более того, Александр Фролов (первый заместитель начальника Главного управления уголовного розыска МВД России) высказывал мнение о том, что на заключенных, находящихся в исправительных учреждениях, приходится треть всех мобильных мошеннических действий.

В 2015 г. заключенные совершили более 1,2 тыс. мобильных преступлений. В 2018 г. ущерб, причиненный гражданам в результате «тюремного» мобильного мошенничества, составил 24 128 500 руб. В 2020 г. ущерб от подобного рода преступлений достиг суммы в 1,8 млрд руб.

В части стабилизации обстановки с «тюремным» мобильным мошенничеством руководством ФСИН России были осуществлены определенные мероприятия:

– установление на территории исправительных учреждений глушилок – это устройства для подавление сотовой связи, то есть генераторы радиопомех (радиоволн разной частоты), в результате работы которых создается «белый шум», существенно снижающий качество мобильной связи. Но от них пришлось отказаться, поскольку глушилки оказались слишком сильными и подавляли сотовую связь не только на территории учреждения, но и далеко за ее пределами. За время использования в исправительном учреждении глушилок поступило огромное количество жалоб в суд и прокуратуру от граждан, проживающих вблизи от исправительного учреждения, на плохую работу сотовой связи и Интернета;

– принятие и применение Федерального закона от 9 марта 2021 г. № 44 «О внесении изменений в отдельные законодательные акты Российской Федерации в части прекращения оказания услуг связи на территории следственных изоляторов и учреждений,

[1] Данное состояние является достаточно устойчивым во времени. Необходимо не менее 48 часов, чтобы потерпевший начал осознавать фактический характер своих действий по перечислению средств преступникам.

исполняющих уголовные наказания в виде лишения свободы» (ФЗ № 44). Однако существенным образом обстановку он не изменил, поскольку проходит достаточно много времени от получения номера сотового телефона, которым пользуются заключенные, до его блокировки операторами связи. Кроме того, заключенные стали применять способы подмены номеров сотовой связи, каналы поступления сотовых телефонов в места лишения свободы остались не перекрыты [3].

2. Недостаточный уровень компетенций сотрудников полиции в сфере информационных технологий, а также низкий уровень технической оснащенности подразделений органов внутренних дел (ОВД), обеспечивающих расследование и раскрытие мобильного мошенничества

Мобильное мошенничество – это новый вид преступлений, которые реализуются в сфере IT-технологий. Расследование и раскрытие подобных преступлений требует наличия у сотрудников специальных компетенций в сфере IT-технологий. Как показывает опыт, в ряде случаев у сотрудников ОВД отсутствуют базовые представления об исследовании цифровых доказательств, о форензике (от англ. *foren science* – судебная наука) – компьютерной криминалистике, методах поиска, получения и закрепления таких доказательств, о мобильной криминалистике и т. п. Сотрудники ОВД, не имея достаточных знаний и компетенций в сфере IT-технологий, не принимают во внимание технические возможности средств сотовой связи по хранению в них текстовой, звуковой информации, фото- и видеозаписей, сведений о входящих и исходящих телефонных номерах, содержание SMS-, EMS-, MMS-сообщений, что приводит к существенному сужению доказательственной базы уголовного дела. Вследствие недостаточной профессиональной подготовки в сфере IT-технологий сотрудники полиции не имеют даже элементарных представлений, как и с помощью чего совершаются киберпреступления, как осуществляется выявление и фиксация криминалистически значимой информации, имеющейся на жестких дисках, смартфонах, планшетах, флешкартах, на которых может храниться информация в электронном виде. В большинстве своем у сотрудников отсутствуют практические навыки извлечения и анализа данных из современных цифровых источников: от мобильных устройств и персональных компьютеров до облачных сервисов, а также знаний, как можно восстанавливать удаленную информацию, эффективно анализировать полученные результаты извлечения. Низкий уровень профессиональной подготовки сотрудников ОВД в сфере IT-технологий не позволяет эффективно расследовать мобильное мошенничество.

В качестве примера рассмотрим технологию осуществления экспертизы устройств подвижной мобильной связи. Изъятые мобильные устройства подвижной мобильной связи направляют в экспертно-криминалистические центры (ЭКЦ), где извлекается доказательственная и ориентирующая информация. Для проведения технической экспертизы мобильных устройств подвижной мобильной связи необходимо:

– вместе с сопроводительным документом предоставить устройство подвижной мобильной связи в ЭКЦ (в зависимости от местоположения ОВД это может занять большое количество времени);

– очередность – ожидание результатов проведения экспертизы (в зависимости от загруженности ЭКЦ она может составить 30–40 суток, при очень большой «настойчивости» – 14 суток). Сама экспертиза (процесс снятия информации с устройства подвижной мобильной связи) при наличии оборудования, программного обеспечения и знаний занимает для кнопочных сотовых телефонов от 5 до 15 мин, для смартфонов – 15 мин;

– получение результатов исследования (в зависимости от местоположения ОВД это может занять большое количество времени).

Технология (порядок проведения) экспертизы устройств подвижной мобильной связи очень времязатратная, все этапы проведения экспертизы устройств подвижной мобильной связи существенным образом замедляют проведение расследования. Возбужденные уголовные дела приходится приостанавливать (в соответствии со ст. 208 УПК РФ), потом возобновлять. Задержанных лиц (в соответствии со ст. 91 УПК РФ) приходится освобождать, затем снова осуществлять розыск и задержание. Эта трата времени, сил и средств оказывает негативное влияние на расследование и раскрытие мобильного мошенничества.

3. Недостаточное участие банковского сообщества России в мероприятиях, направленных на противодействие мобильному мошенничеству

Банковское сообщество России в настоящее время представлено 324 банками. Несмотря на большие прибыли, отечественные банки не стремятся развивать и совершенствовать систему безопасности вкладов клиентов и особенно систему интернет-банкинга. Банковское сообщество напрямую не заинтересовано в поддержке граждан и государства. Этим объясняется отсутствие инициативы в том, чтобы активно консолидироваться с правоохранительными органами в вопросах противодействия киберпреступности [1]. Безопасность вкладов клиентов не является приоритетной задачей в деятельности банков, в основном риски при утрате денежных средств с банковской карты возложены на клиента банка, в договоре дистанционного банковского обслуживания заложена ответственность клиента за потери вследствие разглашения конфиденциальных сведений о банковской карте. Но в связи с отсутствием со стороны банков организации систематической и массовой работы по информированию и обучению населения у клиентов в большинстве случаев нет четкого понимания, что именно относится к конфиденциальным сведениям, какие сведения можно сообщать сотруднику банка по телефону и какие категорически нельзя, что имеет право спрашивать сотрудник банка и т. п. [1].

Отчасти использование преступниками «социальной инженерии» в некотором роде подтолкнуло банковское сообщество к тому, чтобы активизироваться в вопросах противодействия мобильному мошенничеству, поскольку жертвы, находящиеся в состоянии «порока воли», стали оформлять на себя кредиты и переводить их преступникам. Но эти кредиты относятся к категории «плохие кредиты», то есть убыточные, которые не будут выплачены заемщиками. В связи с этим банки стали получать убытки и штрафные санкции. Теперь сотрудники банков более внимательны к лицам, оформляющим кредиты, особенно к их психологическому состоянию. Так, в 2022 г. было предотвращено оформление кредитов на сумму 200 млрд руб.

Из всего банковского сообщества России существенным образом оказывает помощь в борьбе с мобильным мошенничеством Сбербанк. Так, в 2021 г. он содействовал задержанию 94 преступных групп и 4 преступных сообществ, в результате чего было арестовано 510 преступников и получены данные на 8 тыс. чел., которые подозреваются в мобильном мошенничестве [4].

4. Межведомственная разобщенность

Межведомственная разобщенность – это организационная проблема, которая заключается в отсутствии координации в вопросах противодействия мобильному мошенничеству. Она связана с отсутствием механизмов оперативного взаимодействия

(информирования, обмена информацией) правоохранительных органов, банковского сектора; механизмов для оперативного контролирования деятельности операторов связи, интернет-провайдеров и т. п.

Информация по запросам ОВД в связи с расследованием мобильного мошенничества предоставляется операторами связи и интернет-провайдерами по истечении месяца, а иногда не предоставляется вообще.

Анонимность мобильного мошенничества в ряде случаев обусловлена возможностью злоумышленников приобретать и использовать в большом количестве «обезличенные» SIM-карты, оформленные на вымышленных лиц с несуществующими паспортными и анкетными данными, а также на иностранных граждан, которые никогда не пересекали границу Российской Федерации. Это является нарушением законодательства со стороны операторов связи, так как они обязаны идентифицировать абонентов с учетом персонализации. По данному направлению в 2022 г. было составлено 160 административных материалов по ст. 13.29 КоАП РФ. С учетом того что совершается не менее 2 млн телефонных звонков с использованием технологии подмены номера сотового телефона, количество привлеченных к административной ответственности явно недостаточно.

5. Отсутствие эффективного законодательного регулирования процесса борьбы с мобильным мошенничеством

Рассмотрим 2 федеральных закона, регламентирующих борьбу с мобильным мошенничеством в нашей стране. Так, ФЗ № 44 (в части активизации борьбы с «тюремным» мобильным мошенничеством) наделяет руководство территориальных органов УИС полномочиями обращаться к операторам связи с запросом о прекращении оказания услуг сотовой связи в отношении выявленного у заключенных на территории исправительного учреждения абонентского номера. Существенным образом на улучшение обстановки, данный Закон не повлиял. Времени от выявления абонентского номера, используемого заключенными в мошеннических действиях, до его отключения проходит достаточно много, злоумышленники успевают реализовать преступление. Кроме того, заключенными была освоена и получила широкое распространение новая технология SIP-телефонии с подменой абонентского номера за счет изменения параметра CalledID.

Федеральный закон от 24 июля 2023 г. № 369-ФЗ «О внесении изменений в Федеральный закон “О национальной платежной системе”» (ФЗ № 369) сделал попытку преобразовать российскую банковскую систему в части совершенствования банковских технологий при осуществлении интернет-банкинга для повышения уровня безопасности вкладов клиентов. Положения Закона направлены на решение организационной проблемы: разработку совместных действий (механизма) мобильных операторов, банков и государства (в лице правоохранительных органов). В ФЗ № 369 определяется, что «Банк России будет формировать и осуществлять ведение базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента и давать информацию из базы данных операторам по переводу денежных средств, операторам платежных систем, операторам услуг платежной инфраструктуры, операторам электронной платформы».

Новый Закон предлагает осуществлять денежные переводы клиентов с помощью системы «Антифрод», причем они будут проверяться дважды: в банке отправителя и в банке получателя. Банки будут также наделены полномочиями проверять «подозрительные» транзакции и при необходимости приостанавливать их сроком на 2 дня, даже при наличии согласия на перевод клиента. Кроме того, банки обязаны будут возвра-

щать полную сумму украденных средств со счета клиента в течение 30 дней и отключать обслуживание клиента, заподозренного в мошеннических действиях, при наличии информации из правоохранительных органов.

ФЗ № 369 – это первая за 19 лет попытка такого уровня организации эффективной борьбы с мобильным мошенничеством в нашей стране. Но есть некоторые, на наш взгляд, проблемные стороны данного Закона. Так, до 24 июля 2024 г. Банк России должен (только еще) выработать признаки осуществления перевода денежных средств без добровольного согласия клиента и разместить их на своем официальном сайте. Следовательно, в настоящий момент этих признаков нет и как они будут выглядеть, трудно сказать. Кроме того, должен быть разработан механизм и порядок обмена информацией, блокировки счетов и других действий, предусмотренных изменениями в законе и т. п. Насколько эти мероприятия будут эффективными, также сказать сложно.

Предусмотренные ФЗ № 369 мероприятия должны быть осуществлены в обстановке недостаточного участия банковского сообщества в мероприятиях по противодействию киберпреступности. К этому прибавится и то, что банкам придется проработать целый ряд вопросов (в том числе связанных с дополнительными тратами, в ряде случаев существенными), среди которых: организационно-штатные изменения – должны появиться новые структуры, подразделения (отделы), штатные единицы, которые будут реализовывать намеченные в положениях ФЗ № 369 мероприятия; необходимость выполнения требований по компенсированию клиенту денежной суммы операции, осуществленной без его добровольного согласия. У банков появится обязанность реализовывать проверку фактических признаков осуществления перевода денежных средств без добровольного согласия клиента. Конечно, у Банка России есть реальные рычаги воздействия на отечественные банки. Но когда и как будут выполнены положения ФЗ № 369 и насколько они будут эффективными? Насколько банковское сообщество готово к подобного рода новшествам и пойдет ли на них?

В соответствии с ФЗ № 369 «настоящий Федеральный закон вступает в силу по истечении одного года после дня его официального опубликования», то есть 25 июля 2024 г. С учетом сложившихся тенденций роста показателей телефонного мошенничества можно спрогнозировать, что до вступления ФЗ № 369 в законную силу в России будет предположительно совершено более 600 тыс. преступлений, ущерб от которых составит более 22 млрд руб. Очевидно, что в результате реализации мошеннических действий возрастет социальная напряженность в обществе и возникнут вопросы о социальной адекватности ФЗ № 369.

5. Отсутствие международного взаимодействия

По мнению ряда экспертов, способы и технологии совершения киберпреступлений в нашей стране соответствуют европейским десятилетней давности [2]. Вероятно, что в правоохранительных органах европейских стран есть (должны быть) эффективные способы (приемы) противодействия мобильному мошенничеству. Но по понятным причинам рассчитывать на помощь «недружественных стран» (их сейчас более 50) в этом вопросе не приходится. Необходимо отметить, что ряд «недружественных стран» реализовывали свою «недружественную деятельность» задолго до начала СВО. Так, в Эстонии легально разрабатываются сервисы для мошеннической анонимной телефонии Narayana, Black Wolf (с помощью которых осуществляются: подмена телефонных номеров, подмена голоса, защита от определения местоположения, защита от прослушива-

ния, скрытие Imei и т. п.), именно этими сервисами активно пользуются отечественные мобильные мошенники. Координация ряда call-центров осуществляется с территории таких государств, как Германия, США, Нидерланды, Украина [4].

На основании изложенного можно сделать следующие выводы.

Раскрывать рассматриваемые преступления старыми способами, методами, сотрудниками ОВД, не имеющими достаточных IT-компетенций, без достаточной технической оснащенности неэффективно (раскрываемость составляет 19,3–25 %). Это, в свою очередь, и определяет необходимость поиска новых методов, технологий и подходов к раскрытию и расследованию преступлений данного вида.

Отечественные банки (банковское сообщество) должны больше уделять внимания повышению уровня безопасности вкладов клиентов, разработке новых технологий безопасности: банковских карт, банковских операций, банковских платежей, информационной безопасности банковской системы. Необходимо совершенствовать способы контроля за деятельностью операторов связи.

Список источников

1. Копылов В. В., Прокофьев О. М., Калошина Ю. С. Особенности совершения дистанционных хищений денежных средств граждан с использованием метода социальной инженерии // Вестник Московского университета МВД России. 2022. № 3. С. 126–131.

2. Копылов В. В., Анисимова Т. В., Прокофьев О. М. Анализ факторов, способствующих росту киберпреступности в банковском секторе Российской Федерации // Вестник Московского университета МВД России. 2021. № 5. С. 172–176.

3. Копылов В. В., Прокофьев О. М. Перспективы применения криминалистической техники для изучения и анализа данных мобильных устройств в учреждениях ФСИН России // Вестник Московского университета МВД России. 2021. № 2. С. 113–116.

4. Оперативно-розыскная деятельность и современность : сб. науч. тр. / под ред. В. С. Овчинского. М. : ИНФРА-М, 2022. С. 176–184.

References

1. Kopylov, V. V., Prokofiev, O. M. & Kaloshina, Y. S. 2022, ‘Features of remote embezzlement of citizens' funds using the method of social engineering’, *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia,* iss. 3, pp. 126–131.

2. Kopylov, V. V., Anisimova, T. V. & Prokofiev, O. M. 2021, ‘Analysis of factors contributing to the growth of cybercrime in the banking sector of the Russian Federation’, *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia,* iss. 5, pp. 172–176.

3. Kopylov, V. V. & Prokofiev, O. M. 2021, ‘Prospects for the use of forensic technology for the study and analysis of mobile device data in institutions of the Federal Penitentiary Service of Russia’, *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia,* iss. 2, pp. 113–116.

4. Ovchinsky, V. S. (ed.) 2022, *Operational investigative activities and modernity: collection of scientific papers,* pp. 176–184, INFRA-M, Moscow.

Информация об авторах

В. В. Копылов – кандидат юридических наук, профессор кафедры тактико-специальной, огневой и физической подготовки;

О. М. Прокофьев – преподаватель кафедры тактико-специальной, огневой и физической подготовки;
А. А. Субботин – заместитель начальника кафедры тактико-специальной, огневой и физической подготовки;
А. А. Истомин – кандидат психологических наук, доцент кафедры физической, огневой и тактико-специальной подготовки.

Information about the authors
V. V. Kopylov – PhD (Law), Professor of Tactical-special, Fire and Physical Training Department;
O. M. Prokofiev – lecturer of Tactical-special, Fire and Physical Training Department;
A. A. Subbotin – Deputy Head of Tactical-special, Fire and Physical Training Department;
A. A. Istomin – PhD (Psychology), associate professor of Physical, Fire and Tactical Special Training Department.

Примечание
Содержание статьи соответствует научной специальности 5.1.4. Уголовно-правовые науки (юридические науки).

Статья поступила в редакцию 16.12.2023; одобрена после рецензирования 14.02.2024; принята к публикации 21.05.2024.
The article was submitted 16.12.2023; approved after reviewing 14.02.2024; accepted for publication 21.05.2024.