DOI: http://dx.doi.org/10.21686/2411-118X-2025-3-183-191

Проблемы противодействия преступлениям, совершенным организованными группами (на примере телефонного мошенничества)

В. Ю. Мельников
доктор юридических наук, доцент,
профессор кафедры уголовного процесса и криминалистики
Ростовского института (филиала) ВГУЮ (РПА Минюста России).
Адрес: Ростовский институт (филиал)
ФГБОУ ВО «Всероссийский государственный университет юстиции (РПА Минюста России)»,
344019, г. Ростов-на-Дону, Советская ул., д. 32/2.
E-mail: juliameln@mail.ru

Problems of countering crimes committed by organized groups (using the example of telephone fraud)

V. Yu. Melnikov
Doctor of Law, Associate Professor,
Professor of the Department of Criminal Procedure and Criminalistics
of Rostov Institute (Branch) of the All-Russian State University of Justice.
Address: Rostov Institute (Branch) of the All-Russian State University of Justice,
32/2 Sovetskaya Str., Rostov-on-Don, 344019, Russian Federation.
E-mail: juliameln@mail.ru

Поступила 21.07.2025 Принята к печати 30.09.2025

Аннотация

В статье отмечается, что телефонное мошенничество, совершенное организованными преступными группами, – это одна из линий атак на россиян, методов ведения войны против нашей страны, которая возведена в ранг госполитики. Это делают государственные органы или структуры, преступные сообщества (преступные организации), которые находятся под государственным украинским контролем, в их преступной деятельности принимают участие другие лица на территории России. Подобные действия предназначены для сбора персональных данных граждан, организации виртуальных звонков через sim-box, использования российских номеров, перевода похищенных средств за рубеж. Данное исследование приходит к выводу, что для полного, всестороннего и объективного рассмотрения уголовных дел, связанных с мошенничеством организованных преступных групп, такие дела целесообразно относить, в соответствии с требованиями части 2 статьи 151 Уголовно-процессуального кодекса Российской Федерации, к подследственности следователей Следственного комитета Российской Федерации по статье 210 Уголовного кодекса Российской Федерации при оперативном сопровождении ФСБ Российской Федерации.

Ключевые слова: уголовное законодательство, права и свободы человека и гражданина, коррупция, должностные преступления, мошенничество, соучастие, организованная преступность, телефонное мошенничество, преступные сообщества.

Abstract

The article notes that telephone fraud committed by organized criminal groups is one of the lines of attacks on Russians, methods of waging war against our country, which has been elevated to the rank of state policy. This is done by government agencies or structures, criminal communities (criminal organizations) that are under state Ukrainian control, and other persons in Russia take part in their criminal activities to collect personal data of citizens, organize virtual calls via a sim box, use Russian numbers, and transfer stolen funds abroad. As a result of the research, the author comes to the conclusion that for a complete, comprehensive and objective consideration of criminal cases related to fraud by organized criminal groups, it is advisable to refer such cases, in accordance with the requirements of Part 2 of Article 151 of the Criminal Procedure Code of the Russian Federation, to the jurisdiction of investigators of the Investigative Committee of the Russian Federation under Article 210 of the Criminal Code of the Russian Federation with the operational support of the FSB Russian Federation.

Keywords: criminal law, human and civil rights and freedoms, corruption, official crimes, fraud, complicity, organized crime, telephone fraud, criminal communities.

Проблема соблюдения законности и порядка в деятельности должностных лиц и обычных граждан является чрезвычайно актуальной для России[1]. Большое значение имело принятие Федерального закона от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»[2]. В рамках борьбы с коррупцией важно совершенствовать формы и методы взаимодействия прокуратуры и других правоохранительных органов с судами, органами исполнительной и законодательной власти. Для этого требуется более четкая нормативная регламентация вопросов о порядке подготовки информации и обмена ею, разработке и проведении совместных мероприятий, выполнении принятых решений [5]. Многие авторы сходятся во мнении, что именно коррупция в институтах судебной власти подрывает авторитет суда [3. – С. 63; 4]. Так, А. Р. Андреева отмечает, что проблема коррупции в суде становится сейчас особенно актуальной [1].

По итогам 11 месяцев 2022 г. в стране выявлено около 1,8 млн преступлений. Относительно сопоставимого периода предшествующего года их число сократилось на 1,6%[3]. В ходе расследования уголовных дел сотрудники прокуратуры все чаще выявляют нарушения уголовно-процессуального закона (см. табл.).

В данной статье, в частности, рассмотрим вопросы связей между упомянутой сферой и действиями организованных преступных групп на территории Украины и России.

В. В. Путин отметил, что телефонное мошенничество на Украине – это одна из линий атак на россиян, метод ведения войны против нашей страны, которая возведена в ранг госполитики[4]. Этим занимаются государственные органы или структуры, преступные сообщества (преступные организации), которые находятся под государственным украинским контролем. В их преступной деятельности принимают участие другие лица на территории России, уполномоченные для сбора персональных данных граждан, организации виртуальных звонков через sim-box, использования российских номеров, перевода похищенных средств за рубеж. Всё заканчивается иностранными IP-адресами. Ситуация с распространением кибермошенничества в России стала острой, действовать надо быстро, заявил президент России Владимир Путин. «Ситуация, которую мы обсуждаем, является крайне острой. Ущерб для граждан, а значит и для государства, со стороны телефонных и интернет-мошенников приобрел просто недопустимые размеры, очень большие. Поэтому действовать нужно быстро», – указал он.

Таблица

Наименование показателя	1 мес. 2022 г.	1 мес. 2023 г.	% (+;-)
Всего выявлено нарушений законов, в том числе:	387 880	417 235	7,6
- при приеме, регистрации и рассмотрении сообщений о преступлении	250 368	264 058	5,5
- при производстве следствия и дознания	137 512	153 177	11,4
Внесено представлений и информации об устранении нарушений	6 200	7 927	27,9
Привлечено лиц к дисциплинарной ответственности	10 424	12 446	19,4
Поставлено на учет по инициативе прокурора преступлений, ранее известных, но по разным причинам не учтенных	7 328	7 879	7,5

Глава Центробанка Российской Федерации Эльвира Набиуллина сказала, что крупные российские банки «отбивают» 99% мошеннических атак на граждан, но 1% допущенных нападений

[1] Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. – 2016. – № 1 (часть II). – Ст. 212.

[2] Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» // Собрание законодательства Российской Федерации. – 2020. – № 17. – Ст. 2721.

[3] Официальный сайт Генеральной прокуратуры Российской Федерации. – URL: https://epp.genproc.gov.ru/web/gprf

[4] Путин указал на возведение телефонного мошенничества в ранг госполитики Киева. – URL: https://rutube.ru/video/2ecc19102368f653589e24ac6a8cc923/

может нести миллиардный ущерб[1]. В. Путин подчеркнул, что по мере реализации решений в вопросе борьбы с кибермошенничеством необходимо анализировать правоприменительную практику и вносить в законодательство коррективы[2].

В. В. Путин обратил внимание Генпрокуратуры и Роскомнадзора на эту проблему, поручив рассмотреть блокировку вала звонков с Украины и запрет подмены номеров. Президент поручил Правительству России совместно с ФСБ и МВД разработать меры по блокировке звонков с Украины и из других недружественных стран, совершаемых в преступных целях. Также он поручил разработать иные меры, необходимые для защиты прав и интересов россиян, которые могут пострадать при использовании злоумышленниками современных информационно-коммуникационных технологий.

Сложился стереотип, что чаще всего от киберпреступников страдают люди пенсионного и предпенсионного возраста, однако это не так. В 2024 г. жертвами «сотрудников кол-центров» стали 344 тыс. человек, пенсионеров из них – 23,9%. Чаще всего на уловки мошенников попадают лица в возрасте от 25 до 44 лет. Это молодые, активные люди, пользующиеся различными мессенджерами, маркетплейсами, системами электронных расчетов. Они активные пользователи социальных сетей, где оставляют много личных данных, что делает их уязвимыми для злоумышленников. Чаще других страдают жители городов и регионов с большой плотностью населения и развитой экономикой: Москва, Санкт-Петербург, Московская область, Краснодарский край.

Агентство США по международному развитию (USAID) всегда финансировало мошеннические кол-центры на Украине для ослабления и развала Российской Федерации. С 2022 г. Оно ежемесячно вкладывало по $9 млн в работу украинских кол-центров, которые обманывали клиентов российских банков. Цель вливаний USAID – экономическое ослабление России. Эти же кол-центры киевский режим привлекает для диверсий в Российской Федерации, вербуя через них исполнителей. Для изменения номера мошенники используют идентификатор Caller ID, который отвечает за отображение номера на экране смартфона во время входящего звонка. Услуги распространяются виртуальными операторами. Номер злоумышленники получают российский, а значит, он есть в какой-то базе и кто-то за него отвечает – и эти подменные звонки проходят по российским сетям, хотя преступники не должны иметь такой возможности. Остаются проблемы с привлечением представителями западных спецслужб потерпевших от финансовых махинаций для совершения тяжких преступлений, в частности, поджогов, террористических актов (обещая им возврат денежных средств) и свободой вывода мошенниками похищенных средств на территорию зарубежных государств.

Кто и как организовывает поджоги на территории России? В последнее время в СМИ активно обсуждаются участившиеся случаи поджогов в торговых центрах, отделениях банков и почты, зданиях военкоматов, а также автомобилей сотрудников правоохранительных структур. В качестве организаторов этих диверсий выступили телефонные мошенники. При выяснении обстоятельств любого мошенничества в большинстве случаев источник этой агрессии тем или иным образом оказывается на территории Украины, где за последние десятилетия создано множество кол-центров – они есть практически в каждом городе, а их количество превышает 1,5 тыс. офисов. Больше всего подобных учреждений в бывшем Днепропетровске, который уже окрестили столицей телефонного мошенничества. При этом официальных данных о численности операторов нет, но, исходя из масштабов работ, их количество уже измеряется тысячами.

Большая часть задержанных по обвинению в поджоге – студенты, пенсионеры и безработные. Однако в качестве поджигателей выступают и учителя, и многие другие достаточно образованные россияне. Обрабатывают таких граждан через боты для знакомств, профили в соцсетях или телефонный разговор – в условиях «сливов» персональных данных достать номер с именем не составит труда, а вот их уже хватит для получения более полной информации о человеке.

Также нельзя исключать случаи и просто умелого психологического воздействия на доверчивых лиц, а также желание самих жертв подзаработать. Необходимо не забывать про информационное просвещение граждан/родственников, помогая им в освоении самых простых основ ин-

[1] Крупные банки отражают свыше 99 % мошеннических атак на граждан. – URL: https://ria.ru/20250305/banki-2003251915.html

[2] Путин указал на возведение телефонного мошенничества в ранг госполитики Киева. – URL: https://rutube.ru/video/2ecc19102368f653589e24ac6a8cc923/

формационной безопасности и правил поведения в случае оказания давления. На сегодняшний день сотрудники МВД России и СМИ уже начали сообщать гражданам об опасности ответа на сомнительные телефонные звонки, но не всегда это бывает эффективным.

Минцифры и Роскомнадзор обсуждали введение ограничений на звонки в мессенджерах из-за активности мошенников[1]. Рассматривались два сценария: блокировка голосового трафика только из-за границы и полный запрет на голосовые звонки в мессенджерах. По оценкам компании «МегаФон», доля мошеннических звонков в мессенджерах составляет около 40%, хотя три года назад показатель не превышал 1%[2]. Чтобы ограничить возможности телефонных мошенников, Правительство Российской Федерации внесло изменения в перечень лицензий на оказание услуг связи. Из него исключена лицензия на передачу интернет-данных с наложением голосовой информации. Она позволяла с помощью интернета звонить на стационарный или мобильный телефон. Как отметили в правительстве, такая технология давала возможность мошенникам подменять номера[3]. Решение не должно сказаться на обычных пользователях телефонной связи, а граждане, совершающие звонки через разные мессенджеры, используют специальные программы без выхода на сеть стационарной и мобильной телефонной связи. «Чаще всего такими технологиями пользовались мошенники, поскольку это позволяло подменять номера. Теперь этот вид телефонного мошенничества будет серьезно ограничен», – указано в пресс-релизе правительства. Власти заверили, что это никак не скажется на обычных пользователях телефонной связи. «Теперь этот вид телефонного мошенничества будет серьезно ограничен, поскольку будет исключена возможность присоединения сетей передачи данных к телефонным сетям связи», – заявили в пресс-службе Правительства Российской Федерации.

Для мошенников с Украины IP-телефония – единственный способ подменять номера и звонить россиянам с целью обмана. А объем похищенных денег (часть из которых мошенники отдают ВСУ) достиг, по разным оценкам, суммы в размере не менее 250 млрд рублей. В связи с этим действие IP-телефонии сейчас запрещено у нас, но это коснется звонков внутри *Telegram* или *WhatsApp*[4], потому что они осуществляются внутри этих сервисов. Когда через интернет вам звонят либо на мобильный, либо на стационарный телефон, никаких сторонних подключений, как в случае с IP-телефонией, нет.

В производстве следственного отдела по рассмотрению преступлений на территории обслуживания Следственного управления МВД Российской Федерации по г. Ростову-на-Дону находиться уголовное дело, возбужденное 28 октября 2024 г. на основании заявления по признакам преступления, предусмотренного частью 3 статьи 159 Уголовного кодекса Российской Федерации (далее – УК РФ)[5]. Потерпевший, как и многие наши граждане, попался на уловки мошенников, которые действуют с территории Украины. Хотя дело было возбуждено в отношении группы неустановленных лиц (как и многие подобные дела), потерпевший предполагал, что общался с сотрудниками российской фирмы, так как они по телефону и видеосвязи подтверждали свои данные и направили копии паспортов, чтобы потерпевший мог сверить фото в паспорте с их лицами на экране в момент видеосвязи. Потерпевший позже понял, что столкнулся с хищением своего имущества путем обмана, сразу позвонил в банк, и тот заблокировал банковские счета мошенников, которые, как пояснили сотрудники банка, возможно, не успели получить денежные средства. Требовалось содействие следственных органов и возбуждение уголовного дела, без чего невозможно было вернуть денежные средства, наложить арест на банковские счета. Однако, несмотря на устные и письменные ходатайства в адрес следственных органов, потерпевший каких-либо отве-

[1] Коллективная ответственность топ-мессенджеров. – URL: https://www.kommersant.ru/doc/7401636

[2] Минцифры и Роскомнадзор могут полностью запретить звонки в мессенджерах из-за мошенников. – URL: https://www.iphones.ru/iNotes/mincifry-i-roskomnadzor-mogut-polnostyu-zapretit-zvonki-v-messendzherah-iz-za-moshennikov

[3] Правительство ограничило IP-телефонию. – URL: https://www.rbc.ru/technology_and_media/28/12/2024/676fa3f79a79478edf0ae19d

[4] Деятельность компании Meta Platforms Inc. по реализации мессенджера WhatsApp признана экстремистской и запрещена на территории Российской Федерации.

[5] См. материалы уголовного дела № 124… по признакам преступления, предусмотренного частью 3 статьи 159 Уголовного кодекса Российской Федерации // Архив СУ МВД РФ по г. Ростову-на-Дону.

тов не получил, установить мошенников и вернуть похищенные денежные средства не удалось.

Налицо не просто мошеннические действия отдельных неустановленных лиц, а создание преступного сообщества (преступной организации) в целях совершения одного или нескольких тяжких или особо тяжких преступлений либо руководство преступным сообществом (преступной организацией) или входящими в него (нее) структурными подразделениями, а равно координация действий организованных групп, создание устойчивых связей между ними, разработка планов и создание условий для совершения преступлений организованными группами, раздел сфер преступного влияния и (или) преступных доходов между такими группами. В УК РФ центральный признак – «сплоченность» – в полном объеме не отражает его сути.

Злоупотребление должностными полномочиями относится к числу должностных преступлений [2]. Такой подход к определению понятия «злоупотребления должностными полномочиями» исходит из общего конституционного принципа: осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц (ч. 3. ст. 17 Конституции Российской Федерации)[1]. Есть основание отметить требования Постановления Пленума Верховного суда Российской Федерации от 16 октября 2009 г. № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий»[2].

Согласно открытой информации в СМИ, ФСБ Российской Федерации разоблачила международную сеть кол-центров, занимавшуюся массовым мошенничеством под видом совершения инвестиционных сделок. Уголовные дела возбуждались по признакам состава преступления, предусмотренным статьей 210 УК РФ при действенном оперативном сопровождении ФСБ России. Следователям МВД Российской Федерации, по мнению автора, сложнее бороться с такими преступлениями, когда дела возбуждаются по статье 159 УК РФ. В действиях группы неустановленных лиц, возможно, есть признаки преступления, предусмотренные статьей 210 УК РФ. Для полного, всестороннего и объективного расследования уголовных дел такого типа есть основания относить их, в соответствии с требованиями части 2 статьи 151 Уголовно-процессуального кодекса Российской Федерации, к подследственности следователей Следственного комитета Российской Федерации при оперативном сопровождении ФСБ России.

В условиях СВО поймать зарубежных преступников затруднительно, так как большинство западных стран не общается с Россией по вопросам правоохранительной тематики. Почему взаимодействие между странами в этом вопросе очень важно, показывает простой пример. В 2024 г. в России создали совместную с Белоруссией следственно-оперативную группу. Был выявлен колцентр, «сотрудники» которого обманывали россиян. Белорусские коллеги у себя привлекают преступников к ответственности. Ловят соучастников, обслуживающих криминальные схемы у нас в стране, – это курьеры и дропы. Задача любой страны – сделать всё, чтобы эти преступления были невозможны на территории государства. Дропы – это именно та уязвимая часть, на которую возможно воздействовать, чтобы сделать невозможным вывод денег из России. Они предоставляют данные своих банковских карт третьим лицам. Эти третьи лица собирают деньги у потенциальных жертв по заданию зарубежных преступников и переводят их туда, куда им сказали. По оценкам экспертов, в преступную деятельность по обналичиванию похищенных финансов на территории России вовлечено более 2 млн человек.

Кроме того, преступники начали использовать и новый способ вывода средств. Раньше это всё происходило онлайн, а теперь, когда банки стали более бдительны, преступники перешли на курьерскую схему. Существует такая тенденция: приходят какие-то незнакомые люди, курьеры, и люди отдают им наличными все денежные средства, которые у них есть. Далее на эти деньги покупается «крипта», которая уходит за рубеж.

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) // Собрание законодательства Российской Федерации. – 01.07.2020. – № 31. – Ст. 4398.

[2] Постановление Пленума Верховного Суда Российской Федерации от 16 октября 2009 г. № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий» (с изменениями, внесенными постановлениями Пленума от 24 декабря 2019 г. № 59 и от 11 июня 2020 г. № 7) (ред. от 11.06.2020) // Российская газета. – 30.10.2009. – № 207 (5031).

Технология дипфейков (реалистичная подмена фото-, аудио- и видеоматериалов, созданная с помощью нейросетей) становится серьезной угрозой. По данным из открытых источников, путем применения этого инструмента мошенниками был нанесен ущерб 21% компаний. Самая серьезная угроза – подмена голоса руководителя. С развитием технологий 5G качество дипфейков будет только улучшаться. В Госдуме Российской Федерации на рассмотрении находится законопроект, предлагающий ввести в ряд статей УК РФ дополнительный квалифицирующий признак – совершение преступления с использованием дипфейка. Однако с точки зрения здравого смысла пока под вопросом, включать ли в законопроект слово «дипфейк», потому что тогда придется ввести в законы определение этого нового термина. По большому счету, это подделка – обычное мошенничество плюс искусственный интеллект. Это узкая часть цифровизации, а у нас уже есть ее квалифицирующие признаки и положение, что за использование для совершения преступлений каких-то технологических историй, IT-инструментов предусматривается повышенная мера наказания.

Сегодня при получении мошеннических звонков самый надежный способ – это положить трубку и перезвонить своему руководителю, родственнику или знакомому, которому срочно понадобилась финансовая поддержка или конфиденциальная информация. И лучше делать это путем совершения обычного телефонного звонка, а не через мессенджер.

Методы обмана потерпевших правоохранители называют «сценариями»[1]. Показательны и различные методики налаживания контакта с человеком, к каждой из которой у оператора прописан свой скрипт. Рассмотрим лишь некоторые из них. Мошенники представляются консалтинговой компанией, которая содействует в получении страховых выплат, и предлагают подзаработать путем помощи их клиентам. Сначала мошенники выманивают у своей жертвы денежные средства, а затем либо сами обещают их вернуть за поджог, либо звонят снова, но уже представляются сотрудниками ФСБ России и предлагают отомстить «обманщикам», которые якобы находятся в определенном здании, и чтобы их выманить оттуда, это здание надо поджечь, а наказания за это не последует. Получив доверие жертвы, преступники предлагали ей исполнить таким образом «гражданский долг» – наказать преступников, устроив провокацию.

Самый популярный способ мошенничества – звонки от имени правоохранителей или представителей Центрального Банка Российской Федерации, предлагающих перевести деньги на «безопасный счет». Широко распространены звонки от представителей малых групп Fake Boss: преступники звонят от имени сотрудников вузов или каких-то организаций, вводят в заблуждение и собирают денежные средства, предлагая, например, скинуться на подарок на день рождения начальника.

Не теряет актуальности фишинг, когда пользователи идут по поддельным ссылкам на зеркальные сайты организаций и оставляют там данные своих банковских карт. Очень серьезное направление мошенничества – псевдоинвестиции. Потерпевшим предлагают заняться криптотрейдингом, они вкладывают средства, а по итогу там кроме сайта с оболочкой «биржи» ничего нет. Давлению подвергается и портал «Госуслуги». Преступники связываются с жертвой, выманивают у нее смс-код, меняют права доступа к аккаунту и оформляют кредиты. Распространена также рассылка вредоносных программ, позволяющих злоумышленникам получить полный доступ к мобильному устройству. Это только основные сценарии, всего их около полутора сотен. Как только какой-то из сценариев теряет эффективность, разрабатывается новая методика воздействия на человека. В основе всех историй – утечки информации, т. е. данные, которые или воруют хакеры, или выкладываются самими их владельцами в соцсетях. Залог успеха преступников – личная или конфиденциальная информация о потенциальной жертве.

Человек, например, звонит в свою управляющую компанию и говорит: мне нужно заменить трубу. В течение дня таких заявок поступает много, и администратор формирует из них пул, а потом продает в даркнете, где есть большой криминальный рынок покупок этих утечек. Чем он свежее, тем больше шансов обмануть человека. И вот уже на следующий день подавшему заявку на замену трубы начинают звонить преступники: вы подавали такую-то заявку? Дальше все уже

[1] В МВД сообщили, что кибермошенники используют около 1,5 тыс. методов обмана. – URL: https://nova.rambler.ru/search?query=Методы+обмана+потерпевших+правоохранители+называют+«сценариями»

зависит от уровня эрудированности мошенника и уровня образованности и адекватности самого человека. Если он хотел поменять трубу, то зачем ему сообщать куда-то банковские данные? Но и на такие уловки люди попадаются.

Киберпреступность – глобальная проблема, которая наблюдается во всех без исключения странах мира. Только в 2023 г. Интерпол арестовал 3500 человек и 300 млн долларов в 34 странах[1]. В США в 2022 г. сумма похищенных денежных средств составила более 39,5 млрд долларов (или свыше 3 трлн рублей), в Китае – только сумма возмещенных гражданам потерь составила 99,1 млрд юаней (1 трлн рублей).

Госдума Российской Федерации приняла закон о противодействии телефонному мошенничеству[2], который предлагает комплекс следующих мер:

– установка самозапрета через портал «Госуслуги» на дистанционное оформление сим-карт – чтобы их не оформляли злоумышленники;

– установка самозапрета через операторов на массовые обзвоны, чтобы во время телефонного разговора не приходили сообщения от «Госуслуг», в том числе код подтверждения для входа;

– введение обязательной маркировки, которая будет отображать наименование организации при приеме звонков;

– запрет госорганам, банкам, операторам связи на использование зарубежных мессенджеров для общения с клиентами;

– установка запрета на передачу сим-карт третьим лицам при разрешении передачи сим-карт близким родственникам;

– изменение условий оформления сделок: возможность использования биометрии при получении микрозаймов; обязанность банков распространять антифрод-мероприятия не только на онлайн-платежи, но и на банкоматы; создание государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий; введение института уполномоченных представителей клиентов при переводе денежных средств.

Думается, что представленные положения нанесут по кибермошенничеству в том виде, в котором оно существует сегодня, серьезный удар. Понятно, что стопроцентной победы не будет. Этот тип преступлений больше относится к социальной инженерии: убедить человека, что он в каком-то процессе участвует и ему за это надо заплатить. Об эффективности принятого законопроекта пока говорить сложно, потому что сразу добавлено очень много новых опций. Внедрение закона приведет к самому важному – увеличению стоимости афер для мошенников. По большому счету, сейчас это происходит только по одной простой причине: доступ к людям очень дешевый. Теперь же он резко подорожает.

Президент Российской Федерации также утвердил набор поручений по борьбе с цифровыми жуликами[3] для правительства и Центрального банка. Главный акцент – ответственность для банков. Кредитные организации будут вынуждены возвращать клиентам деньги, похищенные с помощью вредоносных программ. Кроме того, и банки, и операторы связи должны будут компенсировать людям потерю средств, если правоохранительные органы выяснят, что организации не приняли необходимых мер для предотвращения преступления. В. В. Путин поручил рассмотреть возможность блокировки учетной записи на портале «Госуслуги» при одновременном изменении двух или более параметров идентификации в личном кабинете, что сильно затруднит деятельность мошенников, переоформляющих на себя аккаунты пользователей для получения кредитов.

В апреле 2025 г. министр развития, связи и массовых коммуникаций Максут Шадаев внес на рассмотрение очередной законопроект по мошенникам,[4] но он касается использования только биометрических систем.

Почему у нас не получалось все это время разобраться с мошенниками? Для этого требует-

[1] Интерпол сообщил об аресте 3,5 тысячи подозреваемых в кибермошенничестве. – URL: https://d-russia.ru/interpol-soobshhil-ob-areste-3-5-tysjach-podozrevaemyh-v-kibermoshennichestve.html

[2] Федеральный закон от 1 апреля 2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации». – URL: https://www.consultant.ru/document/cons_doc_LAW_502182/

[3] «Перечень поручений по итогам совещания с членами Правительства» (утв. Президентом Российской Федерации 01.04.2025 № Пр-706). – URL: https://www.consultant.ru/document/cons_doc_LAW_502304/

[4] Шадаев: осенью в Думу внесут второй пакет мер по борьбе с мошенниками. – URL: https://www.vesti.ru/article/4424990

ся межведомственное взаимодействие, потому что кибермошенничество – это сложная технологическая история. Сперва до человека надо дозвониться, потом задействуется банковская система. То есть на первом месте связь, потом – Центральный банк, где-то там внутри будет проходить МВД, а где-то ФАС.

С одной стороны, если мы боремся за права человека, разве можно запретить снять деньги со своего счета? В принципе банки и так имеют право приостанавливать платежи при сомнительных операциях. Иногда бывают ситуации, когда человеку действительно нужно перевести куда-то крупную сумму. Но, с другой стороны, у нас есть жертвы мошенников, введенные в заблуждение. В течение следующего дня потерпевшие обычно уже что-то понимают, так что им требуется какое-то время для того, чтобы прийти в себя и связаться с родственниками. Учитывая эти ситуации, должен быть выбран некий баланс разумности при введении ограничений на переводы.

Запрет на передачу права пользования номером телефона третьим лицам – хорошая мера. Этот шаг позволит операторам изымать сим-карты, которые очень часто люди отдают в чужие руки. Теперь придется оформлять телефонные номера легально. По вине операторов на рынке был огромный объем серых сим-карт, оформленных на компании. И сейчас встречаются истории, когда люди оформляют на себя, а затем перепродают сим-карты по 500–1000 рублей. Мошенники покупают их у детей, маргиналов, и это та же история, что и с банковскими картами для дропперов – людей, которые помогают жуликам выводить деньги, но теперь есть основание шире привлекать их к ответственности в качестве соучастников.

Таким образом, вводится обязательная маркировка звонков, чтобы было видно, от кого они поступают – от организаций или с международного виртуального номера. Информация станет отображаться на экране телефона. Появится возможность отказаться от рекламных звонков и массовых рассылок, которые делаются без предварительного согласия граждан. Государственным службам, операторам связи, банкам запретят применять иностранные мессенджеры при общении с людьми, подчеркнул премьер. Это поможет пресекать случаи, когда мошенники выдают себя за сотрудников таких учреждений. Для выявления подозрительных действий и их своевременной блокировки планируется создать информационную систему, в которой будут собирать записи голосов тех, кто использует доверие граждан в корыстных целях. Дополнительные меры позволят применять больше инструментов защиты от рисков в цифровой среде. Записи голосов телефонных мошенников будут собираться в специальной информационной системе для идентификации и выявления.

Целесообразно также внести законопроект об использовании средств искусственного интеллекта, за счет прослушивания разговоров граждан которым уровень мошенничества резко упал бы. Азия, Китай и Япония используют эту методику совершенно спокойно. У Минсвязи Российской Федерации есть основание внести закон о разрешении искусственному интеллекту прослушать в отдельных случаях звонки с подозрительных телефонных номеров. Это не все разговоры, поскольку нарушение прав и свободы человека недопустимо. Это крайне эффективный метод борьбы с киберпреступностью. Китай, Япония и Вьетнам внедряют в борьбу с цифровыми мошенниками искусственный интеллект, которому разрешают слушать разговоры и принимать решения.

Полагаем, это только одни из первых шагов по разработке целой системы мер противодействия телефонному мошенничеству.

Список литературы

1. *Андреева А. Р.* Противодействие коррупции в судебной деятельности // Молодой ученые. – 2021. – № 41 (383). – С. 207–209.

2. *Боброва Н. А.*, *Перистый В. В.* Злоупотребление полномочиями как специфическая форма злоупотребления правом // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. – 2020. – № 2 (41). – С. 10–15.

3. *Серегин А. В.* Государственные репрессии против антигосударственного террора: охранительно-правовой опыт обеспечения безопасности России // Проблемы реализации прав человека и гражданина в условиях современных социальных трансформаций : Материалы XIV Всероссийской научно-практической конференции с международным участием, посвященной памяти профессора Ф. М. Рудинского, Москва, 20 апреля 2023 года. – Саратов : Саратовский источник, 2023. – С. 60–64.

4. Судебная власть и судоустройство: тенденции и перспективы правового регулирования : монография / Д. А. Авдеев, М. Т. Аширбекова, А. К. Балдин [и др.]. – М. : Российский университет дружбы народов им. Патриса Лумумбы, 2024.

5. *Цалиев А. М.* О месте и роли судов общей юрисдикции в механизме противодействия коррупции // Вестник Владикавказского научного центра. – 2017. – Т. 17. – № 3. – С. 26–29.