УДК 343.72
ББК 67.408.121.2

ПРОТИВОДЕЙСТВИЕ ТЕЛЕФОННОМУ МОШЕННИЧЕСТВУ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Е. О. Филиппова
Оренбургский государственный университет (Оренбург, Россия)

Статья посвящена анализу современного состояния противодействия телефонному мошенничеству в Российской Федерации. Рассматриваются основные схемы телефонного мошенничества, правовые основы борьбы с данным видом преступлений, технические средства защиты граждан, а также межведомственное взаимодействие в сфере противодействия дистанционным хищениям. Особое внимание уделяется новым технологическим решениям, внедренным в 2024–2025 гг. для защиты граждан от мошеннических действий. Анализируется эффективность принимаемых мер и предлагаются направления совершенствования системы противодействия телефонному мошенничеству.

Ключевые слова: телефонное мошенничество, дистанционные хищения, социальная инженерия, информационная безопасность, киберпреступность, финансовая безопасность, цифровая грамотность, антифрод-системы

COUNTERACTION TO TELEPHONE FRAUD IN THE RUSSIAN FEDERATION

E. O. Filippova
Orenburg State University (Orenburg, Russia)

The article is devoted to the analysis of the current state of counteraction to telephone fraud in the Russian Federation. The main schemes of telephone fraud, the legal basis for combating this type of crime, technical means of protecting citizens, as well as interdepartmental cooperation in the field of counteraction to remote theft are considered. Particular attention is paid to new technological solutions implemented in 2024–2025 to protect citizens from fraudulent activities. The effectiveness of the measures taken is analyzed and directions for improving the system of counteraction to telephone fraud are proposed.

Keywords: telephone fraud, remote theft, social engineering, information security, cybercrime, financial security, digital literacy, anti-fraud systems

Doi: https://doi.org/10.14258/ralj(2025)4.17

Телефонное мошенничество представляет собой одну из наиболее распространенных форм киберпреступности в современной России. По данным МВД России ущерб от действий телефонных мошенников исчисляется десятками миллиардов рублей ежегодно, что делает данную проблему одним из приоритетных направлений работы правоохранительных органов и финансовых институтов страны.

Развитие цифровых технологий и повсеместное распространение мобильной связи создали благоприятную среду для деятельности мошенников, использующих методы социальной инженерии для хищения денежных средств граждан. Преступники постоянно совершенствуют свои схемы, адаптируясь к новым защитным механизмам и используя актуальные информационные поводы для введения граждан в заблуждение.

В России сформировалась комплексная система противодействия телефонному мошенничеству, включающая правовые, организационные и технические компоненты. Центральный банк Россий-

ской Федерации совместно с кредитными организациями внедрил усовершенствованные антифрод-системы, позволяющие выявлять подозрительные операции в режиме реального времени. Введенный в 2024 г. механизм приостановки подозрительных переводов на срок до двух рабочих дней дает возможность банкам провести дополнительную проверку операций и связаться с клиентом для подтверждения транзакции.

Во многих работах ученых юристов подчеркивается необходимость борьбы и предотвращения совершения подобного рода правонарушений, поскольку они подрывают основу конституционного строя Российской Федерации, гарантирующую гражданам страны неприкосновенность частной жизни, и в целом безопасности государства [1, с. 83].

Операторы связи играют ключевую роль в системе противодействия телефонному мошенничеству. С 2025 г. все операторы обязаны использовать технологию определения подмены номера, что существенно затрудняет мошенникам возможность представляться сотрудниками банков или государственных органов. Внедрение системы маркировки звонков позволяет абонентам видеть предупреждение о потенциально опасном звонке еще до ответа на него.

Правовая база противодействия телефонному мошенничеству включает нормы Уголовного кодекса Российской Федерации, предусматривающие ответственность за мошенничество с использованием электронных средств платежа по ст. 159.3 УК РФ [2]. Максимальное наказание по данной статье составляет до десяти лет лишения свободы при особо крупном размере хищения. Кроме того, применяются нормы о мошенничестве в сфере компьютерной информации и общие нормы о мошенничестве.

Межведомственное взаимодействие обеспечивается через специализированные координационные центры, созданные при МВД России и Банке России. Эти структуры осуществляют оперативный обмен информацией между правоохранительными органами, финансовыми организациями и операторами связи. Создание единой базы данных номеров телефонов, используемых мошенниками, позволяет оперативно блокировать их деятельность.

Технологические инновации играют все большую роль в противодействии телефонному мошенничеству. Искусственный интеллект используется для анализа поведенческих паттернов и выявления нетипичных операций. Биометрическая идентификация, внедренная в большинстве крупных банков, существенно усложняет несанкционированный доступ к счетам клиентов.

Важным элементом является формирование культуры безопасного финансового поведения, включающей регулярную смену паролей, использование двухфакторной аутентификации и критическое отношение к любым просьбам предоставить конфиденциальную информацию.

Судебная практика по делам о телефонном мошенничестве демонстрирует тенденцию к ужесточению наказаний для организаторов преступных схем. Суды все чаще применяют дополнительные виды наказаний, включая конфискацию имущества, полученного преступным путем. Возмещение ущерба потерпевшим становится обязательным условием для возможного смягчения наказания.

Анализ следственной и судебной практики позволяет сделать вывод, что наиболее часто с целью завладения денежными средствами потерпевших мошенники выдают себя за:

— попавших в дорожно-транспортное происшествие родственников, обращаясь с просьбой срочно передать денежные средства, чтобы избежать уголовного преследования;
— сотрудников правоохранительных органов (МВД, ФСБ) с просьбой оказать содействие в поимке преступников, которые хотят завладеть денежными средствами потерпевшего;
— сотрудников операторов сотовой связи, говоря о том, что у потерпевшего заканчивается договор с оператором связи и в случае желания его продлить просят сообщить цифровой код из поступившего сообщения, получая тем самым доступ к порталу Госуслуг с конфиденциальной информацией потерпевшего;
— работников банковских организаций с сообщением потерпевшему, как клиенту банка, что на его имя мошенники хотят взять кредит. С целью недопущения противоправных действий предлагают действовать на опережение, сохранив денежные средства потерпевшего путем перевода их на «безопасный счет»;

— работников почтовых отделений, сообщая о поступлении на имя потерпевшего корреспонденции или посылки, для бесплатной доставки которой требуется сообщить цифровой код, поступивший ему в сообщении;
— знакомых, родственников или же руководителей организации работодателя, где потерпевший учится или работает, полностью скопировав личные данные человека, от имени которого пишут, включая фотографию, посредством написания сообщений или звонков в мессенджерах, таких как «Телеграмм», «Вотсап» и др., с просьбой дать денежные средства в долг;
— сотрудников Центробанка России, сообщая, что в ближайшее время выходят денежные купюры нового образца, и необходимо срочно поменять все имеющиеся денежные средства старого (действующего) образца на новые;
— продавцов торговых интернет-площадок (маркетплейсов), которые заинтересовавшемуся товаром покупателю направляют ссылку якобы для оплаты товара, которая ведет на фишинговый сайт [3, с. 45–46].

Это далеко не полный перечень. Список способов обмана постоянно пополняется новыми мошенническими схемами. Об этом регулярно пишут и в СМИ [4].

Роль финансовых организаций в противодействии телефонному мошенничеству постоянно возрастает. Банки инвестируют значительные средства в развитие систем безопасности и обучение сотрудников методам выявления мошеннических операций. Введение обязательного «периода охлаждения» перед осуществлением крупных переводов дает клиентам время обдумать свои действия и при необходимости обратиться за консультацией.

Анализ правоприменительной практики позволяет выделить несколько основных категорий мошеннических схем, получивших распространение в Российской Федерации.

Первую группу составляют схемы, основанные на представлении мошенников сотрудниками банков или государственных органов. Злоумышленники используют технологии подмены номеров, создавая у потенциальных жертв иллюзию звонка от официальных организаций. Под предлогом предотвращения несанкционированных операций или блокировки подозрительных транзакций мошенники получают доступ к конфиденциальной информации и денежным средствам граждан.

Вторая категория включает схемы, эксплуатирующие эмоциональное состояние жертв. Мошенники сообщают о якобы произошедших несчастных случаях с родственниками, необходимости срочной медицинской помощи или юридической поддержки. Создавая атмосферу паники и временного дефицита, преступники добиваются перевода денежных средств без должной проверки полученной информации.

Третью группу образуют схемы, связанные с предложением различных товаров и услуг по привлекательным ценам. Мошенники создают фиктивные интернет-магазины, размещают объявления о продаже товаров, организуют лжеинвестиционные проекты. После получения предоплаты связь с покупателями прерывается, а обещанные товары или услуги не предоставляются.

Правовую основу противодействия телефонному мошенничеству составляет комплекс нормативных актов различного уровня. Уголовный кодекс Российской Федерации содержит ряд составов преступлений, под которые подпадают действия телефонных мошенников.

Профилактическая работа является ключевым элементом системы противодействия телефонному мошенничеству. Повышение уровня информированности населения о типичных схемах мошенничества и способах защиты от них способствует снижению количества успешных преступных посягательств.

Образовательные программы по цифровой и финансовой грамотности должны включать разделы, посвященные безопасному поведению в цифровой среде. Особое внимание следует уделять работе с наиболее уязвимыми группами населения, включая пенсионеров и лиц с ограниченными возможностями здоровья.

Противодействие телефонному мошенничеству в Российской Федерации представляет собой комплексную задачу, требующую координированных усилий государственных органов, финансовых организаций, операторов связи и общества в целом. Несмотря на значительный прогресс в развитии

технических средств защиты и совершенствовании правовой базы, проблема остается актуальной и требует постоянного внимания.

Эффективность противодействия телефонному мошенничеству определяется не только применением передовых технологий и ужесточением наказания для преступников, но и уровнем информированности и бдительности граждан. Формирование культуры безопасного поведения в цифровой среде должно стать приоритетным направлением государственной политики в сфере обеспечения информационной безопасности.

Дальнейшее развитие системы противодействия телефонному мошенничеству должно основываться на принципах комплексности, превентивности и адаптивности к изменяющимся условиям и новым вызовам. Только совместными усилиями всех заинтересованных сторон можно обеспечить надежную защиту граждан от преступных посягательств и создать безопасную среду для развития цифровой экономики и общества.

Видится важность в организации более качественных и эффективных способов контрольных мероприятий. Отметим, контроль выступает основным способом обеспечения законности в государстве [5, с. 187–188].

Ключевыми факторами успеха в борьбе с телефонным мошенничеством являются технологическое развитие защитных систем, повышение финансовой грамотности населения и эффективное межведомственное взаимодействие. Дальнейшее развитие системы противодействия должно учитывать постоянную эволюцию мошеннических схем и необходимость опережающего реагирования на новые угрозы. Только комплексный подход, сочетающий превентивные меры, оперативное реагирование и неотвратимость наказания, способен обеспечить надежную защиту граждан от телефонного мошенничества.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Останина А. М. К вопросу о контрольной деятельности в сфере защиты персональных данных от телефонного мошенничества // Наука. Образование. Современность. 2024. № 1. С. 83–86.

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 31.07.2025). URL: https://www.consultant.ru/document/cons_doc_LAW_10699/

3. Тюхтин Д. А. Противодействие телефонному мошенничеству // Правовой альманах. 2025. № 1. С. 42–47.

4. Бевза Д. Эксперты рассказали о самых популярных мошеннических схемах в 2024 году // Российская газета. 2024. 27 декабря.

5. Останина А. М., Павлов Н. В. Контроль и надзор как основные способы обеспечения законности в административно-публичной деятельности // Евразийский юридический журнал. 2024. № 2. С. 187–188.