Феклисова Арина Владимировна
студентка
ФГБОУ ВО «Санкт-Петербургский государственный
архитектурно-строительный университет»
г. Санкт-Петербург

АНАЛИЗ ТИПОЛОГИЙ ФИНАНСОВЫХ МАХИНАЦИЙ

Аннотация*: автор раскрывает современные тенденции совершения финансовых махинаций, уделяя внимание актуальным формам преступной деятельности в финансовой сфере. В статье определяется необходимость совершенствования механизма предупреждения и пресечения киберпреступлений, посягающих на частную собственность физических лиц.*

Ключевые слова*: киберпреступления, кибербезопасность, финансовые махинации, финансовое мошенничество.*

Актуальность темы научной статьи определяется тем, что в последние годы в России совершается значительное количество киберпреступлений в финансовой сфере. В 2023 г. совершение противоправных деяний в сфере информационных технологий составило 677 тыс. случаев, что на 29,7% больше, чем за аналогичный период 2022 г. Статистика киберпреступлений за январь-август 2024 г. составляет 500,4 тыс. преступлений [4]. Заметим, что основной формой совершения исследуемой группы преступных деяний является кибермошенничество (52,61%). При этом проблемой остается снижение уровня раскрываемости преступлений в сфере информационных технологий. Так, в 2023 г. раскрыто только 37 634 преступлений, что составило 10,56% от общего количества зарегистрированных преступлений в сфере кибермошенничества.

Стратегия национальной безопасности Российской Федерации определяет, что одной из приоритетных угроз, подрывающих государственную и общественную безопасность, является совершение кибермошенничества преступлений посредством использования информационно-коммуникационных технологий.

В научной литературе уделяется внимание вопросам систематизации угроз, подрывающих экономическую и информационную безопасность.

А.К. Моденов и М.П. Власов определяют значимость и первостепенность обеспечения информационной безопасности в условиях цифровизации экономических правоотношений. В подтверждение сказанного авторы указывают, что население активно используют информационные технологии в рамках электронной торговли, что предопределяет необходимость создания легальных инструментов по обеспечению информационной и экономической безопасности. А.К. Моденов и М.П. Власов выделяют две группы угроз, к числу которых отнесены активное вторжение, т. е. искажение и уничтожение информации, а пассивное вторжение, заключающееся в перехвате информации в целях противоправного копирования [1, с. 132].

В.В. Усков, А.В. Макурина, И.С. Завязкина систематизировали угрозы, подрывающие информационную безопасности [3, с. 35]:

– целевые угрозы, под которым следует понимать действия злоумышленников по краже, повреждение информации в целях противоправного получения прибыли;

– нецелевые угрозы, т. е. массовое распространение вредоносных программ, вирусов.

В.В. Усков справедливо указывает, что к приоритетному виду противоправных действий, подрывающих экономическую безопасность, относится мошенничество в сфере кредитования. Однако автором делается вывод о том, что физические лица относятся к наиболее защищенным объектам по причине того, что они в меньшей степени подвергаются мошенническим действиям [2, с. 53–54].

Изучив теоретические основы исследования угроз экономической и информационной безопасности, следует раскрыть вопрос типологии финансовых махинаций.

Рассматривая вопрос типологии финансовых махинаций, необходимо указать, что остается открытым вопрос правового регулирования названных право-

отношений. В подтверждение сказанного укажем, что уголовным законодательством установлены составы кибермошенничества, но не раскрыты способы их совершения. Однако перечнем 25 Указания Генпрокуратуры России №462/11, МВД России №2 от 25.06.2024 г. [5] систематизированы способы совершения киберпреступлений, что позволяет правоохранительным органам обеспечить расследование исследуемой группы преступных деяний. Отметим, что основным недостатком проведенного перечня является отражение узкого понимания отдельного вида кибермошенничества.

В рамках научной статьи проведена систематизация финансовых махинаций. Основным информационным источником явились ресурсы Центрального банка Российской Федерации, отражающие характеристики портрета пострадавшего от кибермошенничества.

Как следует из отчетов, опубликованных Банком России, в Российской Федерации основными формами совершения преступных деяний, посягающих на частную собственность физических лиц, являются фишинг, мошенничество, финансовые пирамиды и безлицензионная деятельность (рис. 1).

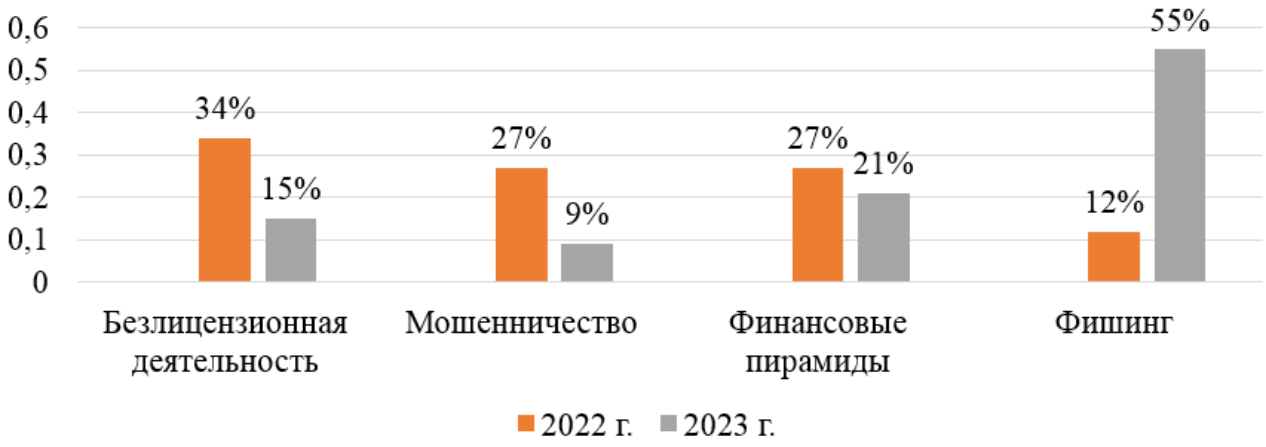

Рис. 1. Ресурсы, используемые злоумышленниками, % [6]

В 2023 г. увеличилось количество совершения противоправных действий, направленных на перевод денежных средств с банковских карт физических лиц без их согласия, что повлекло за собой причинение материального ущерба, равного 1 165,99 млрд руб. (+33,02%).

В 2023 г. было выявлено 984,77 тыс. операций (+662,92%), совершенных посредством использования платежных карт физических лиц без их согласия, что повлекло за собой причинение ущерба в размере 7 120,37 млрд руб. (+353,61%). Основным способом реализации преступной деятельности явилась социальная инженерия, в рамках которой мошенники вынуждали собственников платежных карт совершать перевод денежных средств на нелегальные лицевые и банковские счета.

В 2023 г., как и в 2022 г., увеличилось количество хищений денежных средств физических лиц при оплате товаров и услуг в информационно-телекоммуникационной сети Интернет. Основным инструментом выступила также социальная инженерия, побуждающая потерпевших совершить покупку товара или услуги.

В 2022 и 2023 г. участилось совершение мошеннических действий в рамках дистанционного банковского обслуживания, что повлекло за собой причинение физическим лицам материального ущерба в размере 9 237,51 млн руб.

Таким образом, мошенничество в сфере банковских операций без согласия клиентов-физических лиц относится к одному из приоритетных преступных деяний, посягающих на частную собственность граждан. Сказанное подтверждает вывод о необходимости совершенствования политики по противодействию и предупреждению кибермошенничества посредством проведения мероприятий по повышению финансовой грамотности граждан (в особенности несовершеннолетних, лиц предпенсионного и пенсионного возраста).

Вторым по актуальности совершения кибермошенничества выступает телефонное мошенничество.

В 2023 г. уменьшилось количество финансового мошенничества, совершенного посредством использования телефонных номеров (-23,86%). Сказанное свидетельствует о продуктивной деятельности правоохранительных органов и Банка России по противодействию, пресечению совершения кибермошенничества. Однако остается проблемой увеличения выявленных юридических фактов кибермошенничества посредством использования мобильных телефонных номеров (+0,76% в 2023 г.).

Банком России установлено, что совершение кибермошенничества в форме осуществления звонков от специалистов правоохранительных органов и служб безопасности коммерческих банков, поступающих в целях пресечения противоправного посягательства на денежные средства, размещенные на банковских счетах физических лиц.

Установлено, что участилось совершение звонков с номеров «8–800», что негативно отражается на защите и охране частной собственности граждан (+151,42% в 2023 г.).

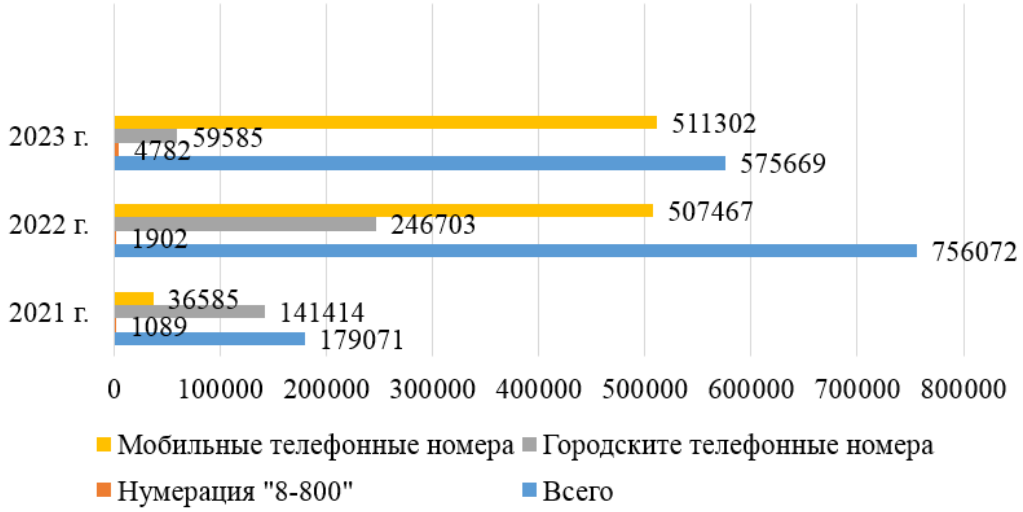

Рис. 2. Количество телефонного мошенничества [6]

Отметим, что основным инструментом телефонного мошенничества выступает социальная инженерия, побуждающая физических лиц совершить следующие действия (рис. 3).

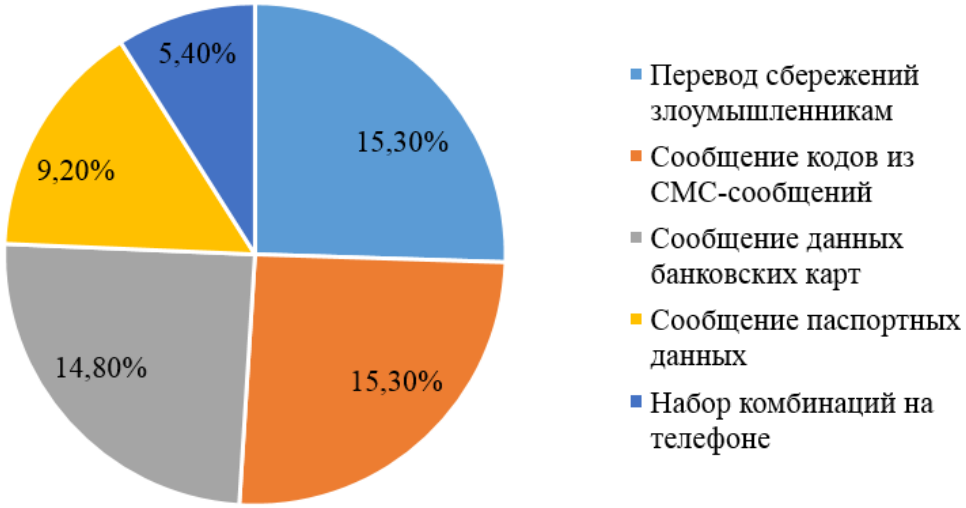

Рис. 3. Действия, совершаемые физическими лицами
в рамках телефонного мошенничества [6]

К следующей группе финансовых махинаций, реализуемых в рамках кибермошенничества, относится фишинг. Указанием Генпрокуратуры России №462/11, МВД России №2 от 25.06.2024 г. определена сущность исследуемого вида финансового мошенничества, заключающаяся в использование злоумышленниками поддельных сайтов (рис. 4). В 2023 г. были выявлены 21 267 (1 951 в 2022 г.) фишинговых Интернет-ресурсов, используемые злоумышленниками в целях противоправного завладения денежными средствами, размещенных на платежных и кредитных картах физических лиц. Банком России инициировано блокирование 4 464 фишинговых интернет-страниц в социальных сетях, что позволило обеспечить защиту от противоправного посягательства на денежные средства граждан.

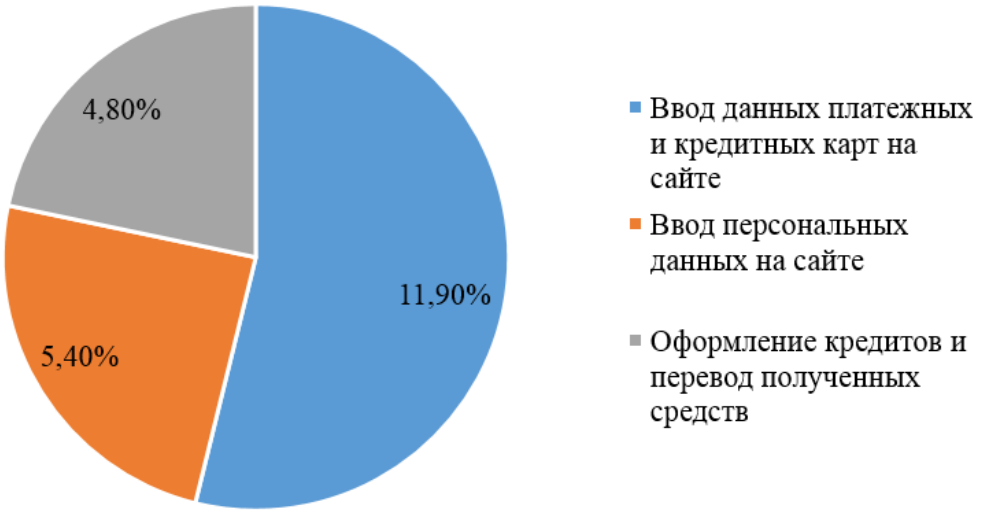

Рис. 4. Действия, совершаемые физическими лицами в рамках использования фишингового (поддельного) интернет-сайта [7]

В России остается проблемой кибермошенничества, совершенной посредством использования финансовых пирамид. Как следует из Указания Генпрокуратуры России №462/11, МВД России №2 от 25.06.2024 г., финансовая пирамида – вид преступного деяния, совершенного в целях противоправного завладения имуществом физических лиц для осуществления производственно-хозяйственной или финансовой деятельности. В 2023 г. доля киберпреступлений, представленных в форме финансовых пирамид, уменьшилась на 6 п. п. и составила 21%. Было выявлено 7 936 (3 923 в 2022 г.) мошеннических ресурсов «Финансовые пирамиды», что повлекло за собой причинение значительного материального имущественного ущерба потерпевшим. Отличительной особенностью названного вида финансовых махинаций является побуждение физических граждан к участию в финансовой деятельности незарегистрированных компаний.

Рассматривая типологию финансовых махинаций, необходимо раскрыть способы их совершения (рис. 5). Социальная инженерия относится к приоритетному способу реализации преступной деятельности, отличительной особенностью которой является оказание психологического воздействия на личность потерпевшего, влекущего за собой добровольное совершение действий по сообщению преступникам данных банковских платежных карт и оформлению кредитных карт в целях последующего перевода денежных средств злоумышленникам.

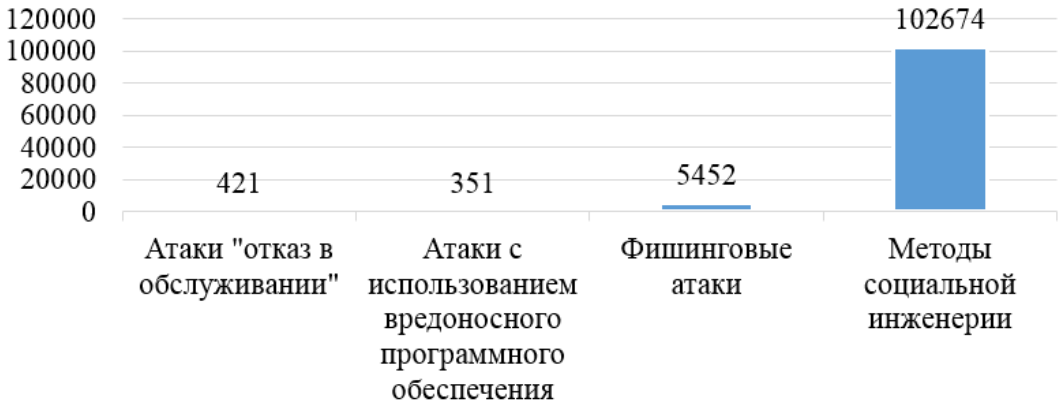

Рис. 5. Способы совершения финансовых махинаций

Обобщая вышесказанное, следует говорить о необходимости совершенствования политики по противодействию и профилактике кибермошенничества посредством информирования населения через средства массовой информации, размещения на общедомовых информационных плакатах основных сведений о мошенниках и способов совершения финансового мошенничества ими с указанием статистических данных, проведение онлайн-мероприятий по повышению финансовой грамотности лиц предпенсионного и пенсионного возраста, несовершеннолетних граждан.

Таким образом, нами сделан вывод о необходимости совершенствования механизма предупреждения совершения кибермошенничества. Приоритетным направлением выступает проведение мероприятий по финансовой грамотности физических лиц, в особенности несовершеннолетних и лиц предпенсионного и пенсионного возраста.

Список литературы

1. Моденов А.К. Особенности экономической безопасности в цифровой экономике / А.К. Моденов, М.П. Власов // Петербургский экономический журнал. – 2020. – №2. – С. 121–134. DOI 10.24411/2307-5368-2020-10015. EDN BPATYU

2. Усков В.В. Комплаенс-контроль в условиях санкций и пандемии как метод обеспечения экономической безопасности / В.В. Усков // Интерактивная наука. – 2022. – №2 (67). – С. 52–55. DOI 10.21661/r-556064. EDN CIHWKT

3. Усков В.В. Информационная безопасность как важнейший компонент оценки рисков в экономической безопасности / В.В. Усков, А.В. Макурина, И.С. Завязкина // Актуальные исследования. – 2022. – №8 (87). – С. 34–36. EDN IUNFHO

4. Состояние преступности в России // Министерство внутренних дел Российской Федерации [Электронный ресурс]. – Режим доступа: https://xn--b1aew.xn--p1ai/reports (дата обращения: 30.10.2024).

5. Указание Генеральной прокуратуры Российской Федерации «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» № 462/11, Министерства внутренних дел Российской Федерации №2 от 25.06.2024 [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1306979238/ (дата обращения: 30.10.2024).

6. Обзор операций, совершенных без согласия клиентов финансовых организаций // Банк России [Электронный ресурс]. – Режим доступа: https://cbr.ru/analytics/ib (дата обращения: 30.10.2024).

7. Кибермошенничество: портрет пострадавшего // Банк России [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/statistics/information_security/ (дата обращения: 30.10.2024).