УДК 343.13

НЕКОТОРЫЕ ВОПРОСЫ СУДЕБНОГО РАЗБИРАТЕЛЬСТВА ПО ДЕЛАМ О МОШЕННИЧЕСТВЕ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Ширяев Антон Вячеславович[1], **Поляков Виталий Викторович**[2]

[1]Троицкий районный суд Алтайского края,
[2]Алтайский государственный университет, Барнаул
av.lex@inbox.ru, agupolyakov@gmail.com

SOME QUESTIONS OF JUDICIAL PROCEEDINGS IN CASES OF FRAUD IN THE FIELD OF COMPUTER INFORMATION

Shiryaev Anton V.[1], **Polyakov Vitaly V.**[2]

[1]Troitsky District Court of the Altai Territory,
[2]Altai State University, Barnaul
av.lex@inbox.ru, agupolyakov@gmail.com

Аннотация. В статье рассматриваются некоторые актуальные проблемы, возникающие при рассмотрении уголовных дел о мошенничестве в сфере компьютерной информации. Отдельное внимание уделено вопросам определения потерпевших по данным преступлениям. Выявлена роль установления действительности кредитного договора и определения реального волеизъявления граждан на осуществление финансовых операций по их счетам. Исследуются практически значимые проблемы судебной практики при оспаривании кредитного договора и банковских транзакций.

Ключевые слова: дистанционное мошенничество, кредитный договор, статус потерпевшего, добросовестность банка, вредоносные компьютерные программы, высокотехнологичные преступления, компьютерные преступления

Abstract. The article examines some relevant issues arising in the examination of criminal cases related to fraud in the field of computer information. Special attention is given to the questions of determining the victims in these crimes. The role of establishing the validity of the credit agreement and determining the genuine intent of individuals to carry out financial transactions on their accounts is highlighted. Practically significant problems in judicial practice when contesting credit agreements and banking transactions are also explored.

Keywords: remote fraud, loan agreement, victim status, bank integrity, malware, high-tech crimes, computer crimes

Для цитирования: *Ширяев А.В. Поляков В.В.* Некоторые вопросы судебного разбирательства по делам о мошенничестве в сфере компьютерной информации // Проблемы правовой и технической защиты информации. 2025. № 13. С. 80–85.

For citation: *Shiryaev A. V. Polyakov V. V.* Some questions of judicial proceedings in cases of fraud in the field of computer information. *Legal and Technical Problems of Information Security*. 2025. No. 13. P. C. 80–85.

На ежегодном заседании Совета при Президенте России по развитию гражданского общества и правам человека был утвержден перечень поручений, в том числе Правительству Российской Федерации совместно с ФСБ России и МВД России, направленных на разработку необходимых мер по защите прав и законных интересов граждан Российской Федерации от преступных посягательств, совершаемых с использованием информационно-коммуникационных технологий[1]. Одним из наиболее распространенных и сложных для расследования противоправных имущественных посягательств в последние годы стали телефонные мошенничества. Эти преступления зачастую входят в криминалистическую группу наиболее опасных высокотехнологичных преступлений [1, 2]. Распространение таких преступных посягательств обусловлено все более выраженной тенденцией изменения общественных отношений, проявляющейся в использовании гражданами цифровых сервисов банковской деятельности [3, с. 3]. Именно это приводит к устремлению преступности в данную сферу, приводит к усложнению средств и способов совершения преступлений, объединения преступников в устойчивые формирования [4].

Согласно данным, которые привел заместитель начальника следственного департамента МВД России Данил Филиппов на Петербургском международном экономическом форуме (ПМЭФ), с января по май 2025 г. в России зафиксировано более 308 тысяч преступлений в IT-сфере, при этом большая часть этих преступлений — дистанционные хищения и мошенничество. Общий ущерб от действий киберпреступников превысил 81 миллиард рублей, и практически все похищенные деньги выводятся в криптовалюту и из юрисдикции России[2]. По статистике Банка России, каждый четвертый похищенный рубль — это заемные средства, т.е. у граждан похищают денежные средства, оформленные в кредит, которые они изначально и не планировали брать у финансовой организации[3].

Одним из важных криминалистических аспектов в расследовании и предупреждении компьютерных преступлений является комплексное исследование специфических особенностей личности потерпевших, поскольку именно эти особенности в значительной мере способствуют преступным посягательствам [5]. При этом УПК РФ положительно разрешил дискуссионный вопрос о возможности признания потерпевшими юридических лиц, что с развитием общественных институтов совершенно обосновано и важно [6]. Однако в науке и практике продолжается полемика о том, кто является надлежащим потерпевшим в отдельных сложных случаях. Так, П.С. Дагель определяет потерпевшего как физическое или юридическое лицо, которому причинен вред (физический, имущественный или моральный) [7, с. 88, 100]. Б.А Протченко. ограничивает потерпевшего только гражданином [8, с. 45]. Для того, чтобы определить, кто является надлежащим потерпевшим по делу — физическое лицо или финансовая организация, необходимо в каждом конкретном случае подробно выяснять все обстоятельства совершенного преступления. По делам о мошенничестве в сфере компьютерной информации, когда выдаче денежных средств гражданину в финансовой организации предшеству-

[1] Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека // kremlin.ru: информационный сайт 07.02.2025. URL:http://www.kremlin.ru/acts/assignments/orders/76233/ (дата обращения: 02.11.2025).

[2] Ущерб от IT-преступлений в России достиг 81 млрд. рублей за пять месяцев // fontanka.ru: информационный сайт 18.06.2025. URL: https://www.fontanka.ru/2025/06/18/75604451/ (дата обращения: 02.11.2025).

[3] Каждый четвертый похищенный мошенниками рубль оказался заемным // vedomosti.ru: информационный сайт 14.02.2024. URL: https://www.vedomosti.ru/finance/articles/2024/02/14/1020233-kazhdii-chetvertii-pohischennii-moshennikami-rubl-okazalsya-zaemnim (дата обращения: 02.11.2025).

ет заключение кредитного договора, который на момент возбуждения уголовного дела в установленном законом порядке не признан недействительным, зачастую потерпевшим по делу признается гражданин — клиент финансовой организации.

При неисполнении своих обязательств заемщиком по кредитному договору, данные обстоятельства порождают гражданско-правовые споры с требованием банка о досрочном возврате кредита заемщиком. Основным доказательством при этом является кредитный договор, заключенный путем акцепта предложения банка через систему онлайн, по условиям которого банк предоставил заемщику кредит, а также встречными исковыми требованиями заемщика о признании кредитного договора недействительным. В последнем случае важными доказательствами являются полученные материалы приостановленного уголовного дела, состоящие, как правило, из протокола осмотра предметов (смартфонов/компьютеров), запросов сотовому оператору, протокола допроса потерпевшего и постановления о приостановлении производства по уголовному делу в связи с неустановлением лица, подлежащего привлечению к уголовной ответственности.

Анализ судебно-следственной практики и экспертных мнений позволил установить, что сложные случаи совершения мошенничества в сфере компьютерной информации, совершаемые в групповой форме, характеризуется весьма высокой латентностью [9, 10]. По тем преступлениям, которые выявлены и дошли до суда, возникают различные трудности судебного разбирательства, связанные с отсутствием единообразной судебной практики. Так, решение суда по гражданскому делу имеет преюдициальное значение для приостановленного уголовного дела, в связи с тем, что при отказе в удовлетворении заявленных требований банка и удовлетворении встречных требований заемщика о признании кредитного договора недействительным, потерпевшим по уголовному делу будет не заемщик, а кредитная организация, которой был причинен ущерб посредством мошеннических действий. Кроме того, для правильного разрешения дела судом, проверки наличия гражданско-правовых отношений между заемщиком и банком и как следствие — оценки статуса потерпевшего по приостановленному уголовному делу важную роль играет способ совершения преступления и действия каждого участника при совершении мошенничества.

Кибермошенничество направлено на получение персональных данных граждан с целью хищения средств с их банковских карт (счетов), обычно через сервисы онлайн-банкинга. При совершении мошенничества в сфере компьютерной информации посредством перевода денежных средств на «безопасный» счет, после сообщения клиентом банка кода подтверждения посторонним лицам сделки оспариваются как совершенные под влиянием обмана потерпевшего третьим лицом. При рассмотрении таких споров особого внимания требует исследование добросовестности и осмотрительности банков, проверки принятых ими мер для оценки реального волеизъявления клиентов на финансовые операции. В частности, к числу обстоятельств, при которых кредитной организации в случае дистанционного оформления кредитного договора надлежит принимать повышенные меры предосторожности, следует отнести факт подачи заявки на получение клиентом кредита и незамедлительная выдача банку распоряжения о перечислении кредитных денежных средств в пользу третьего лица (лиц)[4]. Суды в настоящее время верно обращают внимание на установление добросовестности банков, оценивая, в част-

[4] Определение Конституционного Суда Российской Федерации от 13 октября 2022 года №2669-О // Судебные и нормативные акты РФ: сайт. URL: https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rf-ot-13102022-n-2669-o/ (дата обращения: 02.11.2025).

ности, анализ временных интервалов между подачей заявки и переводом средств, а также поведение сотрудников в подобных ситуациях [11]. Оценивая действия банка при заключении кредитного договора на предмет добросовестности, следует учитывать, приняты ли достаточные меры предосторожности при дистанционном оформлении кредитного договора, обеспечена ли безопасность предоставления услуг, предоставлялась ли информация клиентам в доступной для них форме.

Банк вправе ограничить операции по переводу денежных средств в целях обеспечения безопасности денежных средств своего клиента посредством направления текстового сообщения, однако в силу личного обращения клиента в банк с целью снятия блокировок операций и последующего введения корректных одноразовых кодов банк обязан исполнить распоряжения клиента, данные через мобильное приложение «Онлайн». Однако, к сожалению, на практике на сегодняшний день оснований для признания ненадлежащей идентификации пользователя указанного приложения, не признанного в установленном законом порядке недееспособным, у банка не имеется. Вместе с тем следует отметить, что обязанность банка обеспечивать безопасность при дистанционном банковском обслуживании, не умаляет обязанности самого клиента действовать осмотрительно и выполнять принятые на себя обязательства, в том числе в части обеспечения безопасности при получении банковских услуг.

Кибермошенники все чаще совершают преступления полноструктурным способом, подготавливаясь к преступлениям, маскируя их совершение и скрывая следы-последствия [12, 13]. Зачастую, потерпевшие клиенты банков следуют озвученным по телефону инструкциям неизвестных лиц на протяжении нескольких часов, последовательно совершая действия для получения кредита и в дальнейшем передачи денежных средств преступникам, полагая, что перечисляют денежные средства на «безопасный» счет. В данной ситуации мошенничество в сфере компьютерной информации происходит не одномоментно, что предоставляет возможность как гражданам критически оценить навязываемые им действия, так и банкам удостовериться в реальном волеизъявлении граждан относительно необходимости получения кредитных денежных средств и совершения финансовых операций. Иногда при этом возникает вопрос о том, что у банка имеются сведения о низком доходе заемщика, однако это не свидетельствует о недобросовестности банка, не учитывающего это обстоятельство, поскольку материальное положение относится к риску, который должен учитывать сам заемщик при принятии на себя обязанности по погашению кредита.

В ходе судебного разбирательства все чаще встречаются ситуации, когда при совершении мошенничества в сфере компьютерной информации потерпевшие не вступают в непосредственный контакт с преступниками, при этом оформление кредитного договора, а также осуществление транзакций происходит без их участия. Это осуществляется удаленным образом посредством вредоносных компьютерных программ, занесенных в мобильный телефон или иное пользовательское устройство потерпевших их же неосмотрительными действиями, в том числе при выполнении завуалированных инструкций преступников. В итоге происходит перевод денежных средств потерпевших на счета третьих лиц и участников преступных групп, также производятся дорогостоящие покупки и иным образом выводятся денежные средства потерпевших. Данная ситуация свидетельствует о том, что у потерпевших отсутствовали намерения и выражение волеизъявления на заключение спорного кредитного договора и осуществление иных операций, в связи с чем такой договор и фи-

нансовые операции следует признавать заключенными вопреки воле и интересам потерпевших[5].

Следует отметить, что согласно ст. 147 УПК РФ уголовные дела о преступлениях, указанных в части третьей статьи 20 УПК РФ, возбуждаются не иначе как по заявлению потерпевшего или его законного представителя. Согласно ст. 42 УПК РФ потерпевшим является физическое лицо, которому преступлением причинен физический, имущественный, моральный вред, а также юридическое лицо в случае причинения преступлением вреда его имуществу и деловой репутации. Решение о признании потерпевшим принимается незамедлительно с момента возбуждения уголовного дела и оформляется постановлением дознавателя, следователя, судьи или определением суда.

Возбуждение уголовного дела по заявлению заемщика о хищении у него денежных средств, по которому он признан потерпевшим, не свидетельствует о безусловной недействительности заключенного кредитного договора. Это связано с тем, что данные способы совершения мошенничества не исключают умышленного оформления кредита под видом мошеннических действий как при переводе денежных средств на «безопасный» счет, так и посредством вредоносной компьютерной программы и формального обращения в правоохранительные органы для получения статуса потерпевшего по уголовному делу. Противодействие расследованию со стороны потерпевших может выражаться в уничтожении следов преступления, сокрытии реального ущерба, предоставлении правоохранительным органам только части криминалистически значимой информации и в иных формах [14].

Решение о признании кредитного договора недействительным освобождает потерпевшего от обязательств по оплате задолженности по кредиту, подменяя тем самым предварительное расследование по приостановленному уголовному делу судебным следствием по гражданско-правовому спору. При этом сам факт признания потерпевшим по уголовному делу и вынесение следователем соответствующего постановления подразумевает, что денежные средства были похищены именно у лица, обратившегося с заявлением о хищении денежных средств, существование и принадлежность которых подтверждается наличием кредитного договора, заключенного с банком.

Заемщик, обращаясь в суд с требованиями о расторжении кредитного договора, инициирует разрешение спора в гражданско-правовом порядке, в котором суд, давая оценку представленным доказательствам, опережает ход предварительного расследования по уголовному делу, производство по которому приостановлено, устанавливает юридически значимые обстоятельства, которые могут идти вразрез с обстоятельствами, установленными следователем по делу и доказательствам, полученным криминалистическим путем. Судебная практика по данному вопросу еще продолжает формироваться, а признание онлайн-кредита недействительным остается скорее исключением, чем правилом [15].

Нужно признать, что в большинстве случаев мошенничества в сфере компьютерной информации на сегодняшний день остаются нераскрытыми, порождая как уголовно-правовые, так и гражданско-правовые споры, в частности, направленные на доказывание заключения кредитных договоров и осуществление финансовых операций при реальном волеизъявлении на это граждан, а также установле-

[5] Определение Восьмого кассационного суда общей юрисдикции от 15.10.2025 №88-17011/2025 // Судебные и нормативные акты РФ: сайт. URL: https://8kas.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=34661425&case_uid=c26b14da-2691-4aef-a1c8-d6e40b16f57b&new=2800001&delo_id=2800001 (дата обращения: 02.11.2025).

ние надлежащих потерпевших по данным делам. Настоящее исследование направлено на выявление и анализ ряда проблем судебного разбирательства по делам о компьютерном мошенничестве и возможные пути их разрешения.

Библиографический список

1. Антонян Ю.М. Криминология. 3-е изд., перераб. и доп. М. : Юрайт, 2019. 388 с.

2. Поляков В.В. К проблеме криминалистической сложности расследования высокотехнологичных преступлений // Российский следователь. 2023. № 11. С. 7–10.

3. Ефимова Л.Г., Казаченок О.П., Камалян В.М. [и др.] Цифровое право в банковской деятельности: сравнительно-правовой аспект: монография / отв. ред. Л.Г. Ефимова. М. : Проспект, 2021. 416 с.

4. Поляков В.В. Тенденции развития цифровых средств совершения высокотехнологичных преступлений // Информационное право. 2023. № 4 (78). С. 26–28.

5. Поляков В.В., Ширяев А.В. Криминалистические аспекты личности потерпевших от киберпреступлений // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий / отв. ред. С.И. Давыдов, В.В. Поляков. Барнаул : Изд-во Алт. ун-та, 2018. Вып. XV. С. 164–172.

6. Мисник И.В. Участие потерпевших юридических лиц в уголовном судопроизводстве // Вестник Краснодарского университета МВД России. 2016. № 4 (34). С. 40–43.

7. Фаргиев И.А. Уголовно-правовые и криминологические основы учения о потерпевшем. СПб. : Юридический центр Пресс, 2009. 335 с.

8. Анощенкова С.В. Уголовно-правовое учение о потерпевшем / отв. ред. Н.А. Лопашенко. М. : ВолтерсКлувер, 2006. 248 с.

9. Сухаренко А.Н. Законодательное обеспечение информационной безопасности в России // Российская юстиция. 2018. № 2. С. 2–5.

10. Поляков В.В. Латентность высокотехнологичных преступлений: понятие, структура, методы оценки уровня // Всероссийский криминологический журнал. 2023. Т. 17, № 2. С. 146–155.

11. Макаренко Т.В. Судебная защита прав потребителей финансовых услуг: проблемы и пути совершенствования // Журнал российского права. 2023. № 11. С. 87–96.

12. Кудрявцев В.Н., Эминов В.Е. Криминология / под ред. В. Н. Кудрявцева и В.Е. Эминова. 5-е изд., перераб. и доп. М. : Юристъ, 2014. 800 с.

13. Погодин С.Б. Особенности расследования преступлений в сфере компьютерной информации // Российский следователь. 2004. № 7. С. 6–9.

14. Поляков В.В. Криминалистическая классификация способов противодействия расследованию высокотехнологичных преступлений // Юридическая наука и правоохранительная практика. 2023. № 1 (63). С. 69–79.

15. Клюев А.А. Ответственность банков за действия мошенников при дистанционном обслуживании // Финансовое право. 2023. № 4. С. 61–72.