

УДК 34**Проблемы поиска и доказывания вины онлайн-мошенников в гражданском процессе****Рогацевич Александр Александрович**

Аспирант,
Челябинский государственный университет,
454001, Российская Федерация, Челябинск,
ул. Братьев Кашириных, 129;
e-mail: Rogatsevich@mail.ru

Аннотация

В статье рассматриваются актуальные проблемы поиска и доказывания вины онлайн-мошенников в гражданском процессе. Анализируются правовые аспекты борьбы с онлайн-мошенничеством, включая сложности, связанные с анонимностью в Интернете, юрисдикционными вопросами и представлением цифровых доказательств в суде. Особое внимание уделено проблемам достоверности и допустимости цифровых доказательств, а также пробелам в законодательстве, осложняющим процесс привлечения онлайн-мошенников к ответственности. В статье предложены рекомендации по совершенствованию правового регулирования и судебной практики в целях повышения эффективности борьбы с онлайн-мошенничеством.

Для цитирования в научных исследованиях

Рогацевич А.А. Проблемы поиска и доказывания вины онлайн-мошенников в гражданском процессе // Вопросы российского и международного права. 2024. Том 14. № 11А. С. 233-239.

Ключевые слова

Онлайн-мошенничество, гражданский процесс, доказывание вины, цифровые доказательства, правовое регулирование, судебная практика, анонимность в Интернете, юрисдикция.

Введение

В последние годы с ростом цифровых технологий и Интернета значительно возросло количество преступлений, совершаемых в виртуальной среде. Одним из наиболее распространенных и сложных для преследования преступлений является онлайн-мошенничество. В отличие от традиционных форм мошенничества, действия злоумышленников в цифровом пространстве часто остаются незамеченными или их трудно отследить, что создает серьезные проблемы для правоприменительной практики. Проблема поиска и доказывания вины онлайн-мошенников становится все более актуальной в современном гражданском праве, так как традиционные методы расследования и доказывания не всегда эффективно работают в цифровой среде. Анонимность, глобальность и техническая сложность таких преступлений требуют нового подхода и совершенствования существующих правовых механизмов.

Цель данной статьи – определить основные задачи и предложить решения, необходимые для эффективного поиска и доказывания вины онлайн-мошенников в рамках гражданского процесса. В ходе исследования будут рассмотрены правовые аспекты борьбы с онлайн-мошенничеством, проанализированы сложности, связанные с доказательством вины в суде, а также выявлены ключевые пробелы в действующем законодательстве и правоприменительной практике.

Задачи исследования включают:

1. Исследование правовых аспектов поиска онлайн-мошенников, включая проблемы юрисдикции и анонимности.
2. Анализ сложности доказывания вины в гражданском процессе, связанной с использованием цифровых доказательств.
3. Выявление пробелов в законодательстве и практике, которые затрудняют эффективное преследование онлайн-мошенников.

Настоящая статья направлена на развитие теоретических и практических основ борьбы с онлайн-мошенничеством и формирование предложений по совершенствованию правоприменительной практики в данной сфере.

Основная часть

Онлайн-мошенничество представляет собой одну из форм мошеннических действий, совершаемых с использованием информационно-коммуникационных технологий (ИКТ), в первую очередь сети Интернет. В отличие от традиционных форм мошенничества, которые осуществляются в физическом мире и требуют непосредственного контакта между преступником и жертвой, онлайн-мошенничество характеризуется дистанционностью и анонимностью. В этом контексте онлайн-мошенничество можно определить как незаконное деяние, направленное на получение материальной или иной выгоды обманом путем посредством использования сети Интернет и других цифровых средств.

Классификация онлайн-мошенничества может быть представлена по различным критериям. В зависимости от используемых методов, можно выделить следующие виды.

Фишинг – мошенничество, связанное с обманом получением конфиденциальной информации (пароли, номера банковских карт и т.д.) путем имитации официальных сайтов или организаций.

Вишинг – разновидность фишинга, реализуемая посредством телефонных звонков или

голосовых сообщений.

Скейминг – использование поддельных веб-сайтов и онлайн-платформ для обмана пользователей с целью хищения их средств.

Социальная инженерия – использование психологических методов манипуляции для получения доступа к конфиденциальной информации или ресурсам.

Кибермошенничество в сфере электронной коммерции – мошенничество, связанное с поддельными интернет-магазинами, ложными предложениями о продаже товаров или услуг.

Особенностью онлайн-мошенничества является его массовость и быстрота распространения, обусловленные глобальным охватом Интернета. Кроме того, преступники могут действовать из разных юрисдикций, что усложняет их поиск и привлечение к ответственности. Онлайн-мошенничество также характеризуется высокой степенью адаптивности: преступники быстро меняют тактику и используют новые методы, чтобы избежать обнаружения.

Борьба с онлайн-мошенничеством требует соответствующего правового регулирования как на национальном, так и на международном уровне. В Российской Федерации правовая основа для преследования онлайн-мошенничества заложена в ряде нормативных актов, таких как Уголовный кодекс РФ, Гражданский кодекс РФ, а также законы, регулирующие деятельность в сфере ИКТ.

На международном уровне борьба с онлайн-мошенничеством осуществляется в рамках различных соглашений и договоров, таких как Конвенция Совета Европы о киберпреступности (Будапештская конвенция), которая определяет основные понятия и принципы борьбы с преступлениями, совершаемыми с использованием компьютерных технологий. Международные правовые акты направлены на гармонизацию законодательства стран-участников, что позволяет более эффективно преследовать преступников, действующих в различных юрисдикциях.

Особое внимание в правовом регулировании уделяется вопросам сбора и использования цифровых доказательств, что отражено в процессуальных кодексах и специальных актах. Несмотря на наличие правовых норм, регулирующих борьбу с онлайн-мошенничеством, существуют значительные проблемы в их применении на практике. Это связано как с быстрым развитием технологий, так и с особенностями интернет-пространства, которые требуют гибкости и адаптивности от правоприменительных органов.

Одной из основных сложностей в борьбе с онлайн-мошенничеством является анонимность, которую предоставляют злоумышленникам современные технологии. Преступники могут использовать виртуальные частные сети (VPN), анонимайзеры, поддельные IP-адреса и другие средства, позволяющие скрыть их личность и местоположение. Это значительно затрудняет процесс их обнаружения и идентификации.

Еще одной проблемой является юрисдикционная сложность. Онлайн-мошенники могут действовать из разных стран, находящихся в разных юрисдикциях, что затрудняет международное сотрудничество правоохранительных органов. В таких случаях требуется согласование действий между различными странами, что требует значительного времени и усилий. Процедуры экстрадиции и международной правовой помощи часто осложняются различиями в правовых системах и подходах к преследованию онлайн-преступлений.

Использование технических средств для поиска и доказательства вины онлайн-мошенников также сопряжено с рядом трудностей. Проблемы возникают не только на этапе сбора цифровых доказательств, но и на этапе их оценки в судебном процессе. Вопросы достоверности и

допустимости таких доказательств часто вызывают споры, особенно в тех случаях, когда методы их получения не полностью соответствуют требованиям процессуального законодательства.

В процессе установления вины онлайн-мошенников в гражданском процессе особое значение приобретает доказательственная база, включающая различные виды цифровых доказательств. Среди наиболее часто используемых видов доказательств можно выделить следующие.

Цифровые следы – данные, оставленные мошенником в ходе его действий в Интернете, такие как журналы активности на веб-сайтах, записи логов серверов, информация о транзакциях и других операциях. Эти следы позволяют проследить маршрут действий преступника и установить его личность. Например, в исследованиях А.Д. Еремеевой анализируется использование цифровых следов для выявления подозреваемых в кибермошенничестве, что подтверждает эффективность этого метода при условии наличия достаточных технических ресурсов [Еремеева, 2020].

Переписка – сообщения, передаваемые через электронную почту, мессенджеры или социальные сети. В работе Е.Н. Бархатовой указывается на важность анализа содержания переписки, которая может содержать информацию о намерениях, планах и действиях мошенника. Примеры успешного использования переписки в качестве доказательства встречаются в судебной практике, когда мошеннические схемы раскрывались через анализ сообщений, связанных с обманом жертв [Бархатова, 2021].

Вопросы представления и оценки цифровых доказательств в суде являются одними из наиболее сложных аспектов гражданского процесса. Проблемы достоверности и допустимости цифровых доказательств обсуждаются в многочисленных исследованиях, среди которых работа А.Ю. Решетникова занимает важное место. Он подчеркивает, что цифровые доказательства могут быть легко подделаны или изменены, что требует особой осторожности при их оценке [Решетников, Русецкий, 2018].

Судебная практика показывает, что для признания цифровых доказательств допустимыми необходимо соблюдение ряда условий, включая обеспечение целостности данных, правильность их хранения и представления в суде. Например, в делах, рассмотренных в исследовании А.А. Энгельгардта, суды часто отказывались принимать в качестве доказательств скриншоты переписки или другие цифровые данные из-за отсутствия подтверждения их подлинности и происхождения [Энгельгардт, 2019].

Борьба с онлайн-мошенничеством в гражданском процессе сталкивается с рядом значительных проблем, обусловленных недостатками и пробелами в действующем законодательстве и судебной практике. Эти пробелы создают сложности для эффективного преследования и наказания лиц, занимающихся мошенничеством в цифровой среде.

Одной из ключевых проблем является отсутствие четкого определения онлайн-мошенничества в российском законодательстве. В настоящее время понятие онлайн-мошенничества не имеет строгого правового определения, что приводит к разночтениям при квалификации таких деяний. Как отмечает А.Д. Еремеева, отсутствие единого подхода к определению онлайн-мошенничества создает правовую неопределенность, что затрудняет правоприменение и приводит к неоднородной судебной практике.

Еще одной серьезной проблемой является отсутствие специальных норм, регулирующих порядок сбора, хранения и представления цифровых доказательств в суде. Существующее процессуальное законодательство не учитывает специфики работы с цифровыми

доказательствами, что создает препятствия для их эффективного использования в гражданском процессе. В результате суды часто сталкиваются с проблемами достоверности и допустимости таких доказательств, что может привести к отказу в удовлетворении исков [Еремеева, 2020].

Кроме того, законодательство в сфере международного сотрудничества также содержит значительные пробелы, осложняющие борьбу с онлайн-мошенничеством, совершаемым из-за рубежа. А.Ю. Решетников считает, что отсутствие согласованных процедур обмена информацией и взаимодействия между странами существенно затрудняет расследование и преследование преступников, действующих в международной среде. Это приводит к тому, что многие дела, связанные с онлайн-мошенничеством, остаются нераскрытыми или не доводятся до суда.

Наконец, важным пробелом в законодательстве является отсутствие комплексного подхода к защите прав потерпевших от онлайн-мошенничества. А.Ю. Решетникова указывает на недостаточность существующих механизмов компенсации ущерба, причиненного онлайн-мошенничеством. Потерпевшие часто сталкиваются с проблемами возврата похищенных средств и возмещения убытков, что подрывает доверие граждан к системе правосудия [Решетников А.Ю., Русецкий, 2018].

Для повышения эффективности борьбы с онлайн-мошенничеством и устранения существующих пробелов в законодательстве и судебной практике необходимо разработать и внедрить ряд изменений и нововведений.

Первым шагом должно стать введение четкого и унифицированного определения онлайн-мошенничества на законодательном уровне. Это позволит создать единые стандарты квалификации преступлений, связанных с использованием цифровых технологий, и обеспечит единообразие правоприменительной практики. А.А. Энгельгардт предлагает разработать специальный законодательный акт, посвященный борьбе с киберпреступностью, который включал бы детализированные положения о различных формах онлайн-мошенничества [Энгельгардт, 2019].

Вторым направлением совершенствования законодательства должно стать введение специальных норм, регулирующих порядок работы с цифровыми доказательствами. В частности, необходимо разработать процессуальные нормы, устанавливающие требования к сбору, хранению и представлению цифровых доказательств в суде, а также предусмотреть механизмы их проверки на достоверность.

Для решения проблем международного сотрудничества необходимо разработать новые механизмы взаимодействия между странами в области борьбы с онлайн-мошенничеством. В частности, следует активизировать работу по заключению двусторонних и многосторонних соглашений о сотрудничестве в сфере обмена информацией, экстрадиции и совместного расследования преступлений. В исследовании Е.Н. Бархатовой предлагается создание международной базы данных по киберпреступлениям, которая позволила бы оперативно выявлять и преследовать преступников, действующих на международном уровне.

Наконец, для защиты прав потерпевших необходимо разработать комплексные меры по компенсации ущерба, причиненного онлайн-мошенничеством. Предлагается создание специального фонда компенсации для потерпевших, который финансировался бы за счет конфискованных у мошенников средств и взносов от крупных интернет-компаний. Это позволит более эффективно защищать права граждан и восстанавливать справедливость в случаях онлайн-мошенничества [Бархатова, 2021].

Внедрение данных рекомендаций потребует активного взаимодействия между

законодательными органами, судебной системой и международными организациями. Только комплексный и координированный подход позволит эффективно бороться с онлайн-мошенничеством и защитить интересы граждан в цифровую эпоху.

Заключение

Таким образом, из всего вышесказанного можно сделать вывод, что в условиях стремительного развития цифровых технологий проблема поиска и доказывания вины онлайн-мошенников в гражданском процессе становится все более актуальной. Проведенный анализ показал, что существующее законодательство и судебная практика сталкиваются с серьезными вызовами, связанными с анонимностью преступников, сложностями в сборе и оценке цифровых доказательств, а также пробелами в международном сотрудничестве. Для эффективного противодействия онлайн-мошенничеству необходимо разработать и внедрить новые правовые механизмы, направленные на улучшение процесса доказывания и защиты прав потерпевших. Введение четких правовых норм, регулирующих работу с цифровыми доказательствами, и активизация международного сотрудничества являются ключевыми направлениями для повышения эффективности борьбы с этим видом преступлений.

Библиография

1. Бархатова Е.Н. Особенности квалификации мошенничества в сфере компьютерной информации и его разграничение с иными составами преступлений // Современное право. 2021. № 9. С. 89-101.
2. Еремеева А.Д. К вопросу о способах совершения мошенничества в сфере компьютерной информации // Вестник студенческого научного общества ГОУ ВПО «Тюменский национальный университет». 2020. № 12-1. С. 112-115.
3. Кулешова Н.Н., Христофорова Е.И. Особенности квалификации мошенничества в сфере компьютерной информации // Вестник Алтайской академии экономики и права. 2019. № 6. С. 184-188.
4. Решетников А.Ю., Русецкий Е.А. Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации // Гражданское право. 2018. № 2. С. 72-76.
5. Энгельгардт А.А. Вопросы квалификации мошенничества в сфере компьютерной информации // Право. Журнал высшей школы экономики. 2019. № 4. С. 55-62.

Problems of finding and proving the guilt of online fraudsters in civil proceedings

Aleksandr A. Rogatsevich

Postgraduate Student,
Chelyabinsk State University,
454001, 129 Brat'ev Kashirinykh str., Chelyabinsk, Russian Federation;
e-mail: Rogatsevich@mail.ru

Abstract

The article examines current issues of finding and proving the guilt of online fraudsters in civil proceedings. It analyzes the legal aspects of combating online fraud, including the difficulties associated with anonymity on the Internet, jurisdictional issues, and the presentation of digital evidence in court. Particular attention is paid to the issues of the reliability and admissibility of

Aleksandr A. Rogatsevich

digital evidence, as well as gaps in legislation that complicate the process of bringing online fraudsters to justice. The article offers recommendations for improving legal regulation and judicial practice in order to increase the effectiveness of the fight against online fraud.

For citation

Rogatsevich A.A. (2024) Problemy poiska i dokazyvaniya viny onlain-moshennikov v grazhdanskom protsesse [Problems of finding and proving the guilt of online fraudsters in civil proceedings]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 14 (11A), pp. 233-239.

Keywords

Online fraud, civil procedure, proof of guilt, digital evidence, legal regulation, judicial practice, anonymity on the Internet, jurisdiction.

References

1. Barkhatova E.N. (2021) Osobennosti kvalifikatsii moshennichestva v sfere komp'yuternoi informatsii i ego razgranichenie s inymi sostavami prestuplenii [Features of the qualification of fraud in the field of computer information and its distinction from other crimes]. *Sovremennoe parvo* [Modern law], 9, pp. 89-101.
2. Engelhardt A.A. (2019) Voprosy kvalifikatsii moshennichestva v sfere komp'yuternoi informatsii [Issues of qualification of fraud in the field of computer information]. *Pravo. Zhurnal vysshei shkoly ekonomiki* [Law. Journal of the Higher School of Economics], 4, pp. 55-62.
3. Eremeeva A.D. (2020) K voprosu o sposobakh soversheniya moshennichestva v sfere komp'yuternoi informatsii [On the issue of methods of committing fraud in the field of computer information]. *Vestnik studencheskogo nauchnogo obshchestva GOU VPO «Tyumenskii natsional'nyi universitet»* [Bulletin of the student scientific society of the State Educational Institution of Higher Professional Education "Tyumen National University"], 12-1, pp. 112-115.
4. Kuleshova N.N., Khristoforova E.I. (2019) Osobennosti kvalifikatsii moshennichestva v sfere komp'yuternoi informatsii [Features of the qualification of fraud in the field of computer information]. *Vestnik Altaiskoi akademii ekonomiki i prava* [Bulletin of the Altai Academy of Economics and Law], 6, pp. 184-188.
5. Reshetnikov A.Yu., Rusetskii E.A. (2018) Nekotorye voprosy kvalifikatsii neokonchennykh prestuplenii v sfere komp'yuternoi informatsii [Some issues of qualification of unfinished crimes in the field of computer information]. *Grazhdanskoe parvo* [Civil law], 2, pp. 72-76.