

Дата поступления рукописи в редакцию: 02.05.2026 г.

DOI: 10.24412/2782-3849-2026-6-217-221

Дата принятия рукописи в печать: 25.06.2026 г.

АМИНОВ Ильдар Ринатович,

кандидат юридических наук, доцент, доцент кафедры уголовного процесса Уфимского юридического института МВД России,

e-mail: Aminov76@mail.ru

ШАРИПОВА Эльмира Азгаровна,

кандидат философских наук, доцент кафедры финансового и административного права Института права Уфимского университета науки и технологий Республики Башкортостан,

e-mail: elmira.scharipova@yandex.ru

МЕТОДЫ И СПОСОБЫ СОВЕРШЕНИЯ МОШЕННИЧЕСТВА С ПОМОЩЬЮ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

◇ **Аннотация.** Современный этап жизни человечества характеризуется интегрированием цифровых технологий и программных обеспечений на цифровые устройства. Данный аспект несет положительный характер в области упрощения жизнедеятельности человека. Актуальность выбранной темы работы заключается в появлении и стремительном распространении в преступном мире технологии Искусственного интеллекта (далее ИИ). Автором проанализированы и выделены методы и способы совершения мошенничества с использованием искусственного интеллекта.

◇ **Ключевые слова:** Искусственный интеллект, технологии, мошенничество, способы, информация, преступность, потерпевший.

AMINOV Ildar Rinatovich,

Candidate of Law, Associate Professor Associate Professor of the Department of Criminal Procedure, Ufa Law Institute of the Ministry of Internal Affairs of Russia

SHARIPOVA Elmira Azgarovna,

Candidate of Philosophical Sciences, Associate Professor, Department of Financial and Administrative Law Institute of Law Ufa University of Science and Technology of the Republic of Bashkortostan

METHODS AND WAYS OF COMMITTING FRAUD USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

◇ **Annotation.** The modern era of human life is characterized by the integration of digital technologies and software onto digital devices. This aspect has a positive impact on simplifying human life. The relevance of this topic lies in the emergence and rapid spread of Artificial Intelligence (hereinafter AI) technology in the criminal world. The author analyzes and highlights methods and ways of committing fraud using artificial intelligence.

◇ **Key words:** Artificial intelligence, technology, fraud, methods, information, crime, victim.

Российское общество претерпевает масштабные изменения, связанные с повсеместным внедрением цифровых технологий. Цифровизация российской экономики привела к росту киберпреступности. Согласно статистике МВД РФ, за восемь месяцев 2024 года зафиксировано более полумиллиона правонарушений с применением ИТ-технологий [1].

Появились новые схемы мошенничества,

поэтому в настоящее время следует быть бдительным и очень внимательным при совершении различных действий с использованием электронных устройств, особенно если это касается выполнения электронных платежей. Ведь при недостаточной осведомленности интернет-пользователь рискует попасть в очень сложное положение, потерять свои финансы или столкнуться с утечкой информации, своих персональных данных [2].

В науке уголовного права и криминалистики способ и метод совершения преступления занимает одну из важных составляющих в системе криминалистической характеристики преступного деяния, именно данные элементы характеризуют природу самого деяния, особенности личности преступника и специфику предмета преступного посягательства. Исследование способов и методов совершения мошенничества с использованием информационно-телекоммуникационных технологий несет в себе необходимый характер, вследствие стремительной цифровой трансформации в мире, злоумышленниками разрабатываются новые схемы совершения данной категории преступлений.

В современной уголовно-правовой доктрине выделяется, что применение информационно-телекоммуникационных технологий при совершении мошенничества могут выполнять различные функции. Ученый-правовед Галашина Е.А., в своей работе «Мошенничество с применением информационных технологий: уголовно-правовая оценка», выделяет две функциональные составляющие при применении информационных технологий для совершения мошенничества:

В одних случаях, информационные технологии используются мошенниками как средство связи с населением, для осуществления своих корыстных целей. В основном злоумышленниками используют методы социальной инженерии (представляются сотрудниками банковских организаций, сотовых компаний или интернет-провайдерами), которые применяются с помощью информационно-телекоммуникационных технологий.

В других случаях, цифровые устройства являются инструментом для вторжения и вмешательства в компьютерные процессы и кибер-среду, что предопределяет другую юридическую значимость, то есть, в данном случае, будет совершение других составов преступления, например, деяния, перечисленные в главе 28 «Преступления в сфере компьютерной информации» Уголовного кодекса РФ.

Анализируя научные работы, посвященные тематике цифрового мошенничества, необходимо отметить, что доминирующее положение из способов совершения данного преступного деяния, является использование методов социальной инженерии, основанные на психологическом манипулировании над потерпевшими, путем вторжения к ним в доверие или оказания психологического давления, например, запугивание или прямые угрозы. Согласно статистическим данным МВД России за последние 3 года, уровень мошенничества

с применением цифровых технологий растет. При этом наблюдается устойчивое усложнение способа совершения деяния: мошенники активно используют темы, вызывающие у потерпевших лиц острые эмоции, например, затрагивают вопросы утраты личных сбережений с банковских счетов или здоровье и жизнь близких людей.

Примером такого способа совершения мошенничества является звонок мошенником потерпевшему лицу, от лица сотрудника банковской организации. Так, согласно следственно-судебной практике, существует множество случаев, когда лица, осуществляющие мошеннические действия, по предварительному сговору, систематически совершают данные телефонные звонки, с схожим содержанием, для получения денежных средств, в основном, данная методика работает на пожилую категорию граждан РФ. Под предлогом проведения проверочных мероприятий или предотвращению хищений, они убеждали потерпевших лиц, передать им код, высланный по СМС от имени банковской организации, для получения доступа в аккаунт разрабатываемого лица. В ходе проведения данных действий, банковский счет и интернет-профиль потерпевшего передавался в руки мошенников, где осуществлялись переводы с электронных счетов на другие банковские карты, принадлежавшие злоумышленникам. После получения данных денежных средств, их вкладывают в крипто-кошельки, чтобы передвижение денежных средств было скрыто и личности преступников не были раскрыты.

Особое внимание заслуживает случай, связанные с посягательством мошенниками на недвижимое имущество населения государства. Согласно следственно-судебной практике, в Иркутской области, был зафиксирован случай, когда пострадавшая, действуя по указаниям лица, представившейся сотрудником банковской организации, обратилась в агентство по продаже недвижимости и выставила там свою квартиру на продажу на 4 миллиона рублей ниже рыночной. По изучению данного дела, правоохранными органами была выявлена особенность, связанная с тем, что по данному случаю, не было вмешательства специальных субъектов – риэлторов, занимающихся вопросами сопровождения недвижимого имущества и выставления его на продажу. Данное обстоятельство актуализирует проблему межведомственного взаимодействия правоохранительных органов и риэлторской службы в целях профилактики подобных случаев.

Технологические способы и методы совершения мошенничества с использованием информационно-телекоммуникационных технологий систематически получают свое

развитие и эволюционируют. В настоящее время мошенники используют методику фишинга.

Фишинг – это вид интернет-мошенничества, при котором злоумышленники пытаются заполучить персональные данные, содержащую в себе логины и пароли от аккаунтов, реквизиты банковской карты или другую любую информацию населения, путем отправки «ложных» интернет-сайтов известных компаний, например, сайт коммерческой банковской организации «Сбербанк». Ложность сайта заключается в том, что злоумышленники создают специальный скрипт или код, вживляемый в их созданный сайт. Данная интернет-страница ничем не отличается от «оригинального» сайта организации. Переходя по полученной ссылке, человек сталкивается с авторизационным окном, где пользователь вводит свой логин и пароль для входа на страничку. Далее, получив эти данные, злоумышленник получает доступ к кабинету потерпевшего лица и тем самым мошенник может в свободном доступе, от имени пострадавшего лица, осуществлять любые действия.

Отличие фишингового-сайта от оригинального заключается в том, что мошенники могут добавить лишний символ в гиперссылку, например, поставить точку или написать вместо русской буквы английскую, тем самым поменяв символ в интернет-ссылке. Данная процедура происходит, так как домен настоящего сайта организации запатентован и находится в базе данных реестра интернет-ссылок РФ, вследствие этого, злоумышленники, для обхода данной системы, переделывают гиперссылку и преподносят её в виде «оригинального» интернет-сайта населению, чтобы заполучить их персональные данные [4].

Следующим из распространенных методов используемый мошенниками является – Вишинг. Понятие «Вишинг» встречается во многих научных работах, посвященных интернет-мошенничеству. Так, в работе научного деятеля Куренной В.О. «Фишинг и вишинг в информационной безопасности», данное понятие она раскрывает в таком виде: «Вишинг – (голосовой фишинг) является одним из способов совершения интернет-мошенничества, при котором злоумышленники используют телефон как средство совершения преступного деяния». Необходимо отметить, что вишинг, в своем роде, является одним из самых передовых способов совершения преступления, так как никаких дополнительных затрат и трудностей мошенникам не предоставляется, используя данный метод. Преступники совершают массовые телефонные звонки населению каждый день, с целью обмана или злоупотребления доверием заполучить интересующую их информацию,

например, персональные данные пользователей сети-интернет, реквизиты банковских карт и счетов или личную информацию о лице. Получив эти данные, злоумышленники могут заполучить денежные средства, путем угрозы распространения личной информации в сети-интернет или шантажировать пользователей, к примеру, угрозой блокировки банковских счетов и карт. Как правило, мошенники представляются сотрудниками банковских организаций и сообщают информацию о том, что с банковской карты клиента списаны денежные средства, с целью противодействия дальнейшим незаконным переводам, злоумышленник просит данные от банковского аккаунта пользователя, с целью осуществления корыстных целей.

Необходимо отметить, что одним из новейших способов совершения данной категории преступления является мошенничество в сфере инвестиций. Согласно следственно-судебной практике и статистике МВД России за 2025 год, участились случаи обмана населения государства путем проведения телефонных звонков с предложением заниматься инвестиционной деятельностью. В данном способе пересекаются методики фишинга и вишинга, так как мошенники связываются с клиентами банковских организаций через сотовую связь и предлагают инвестировать в различные проекты или осуществлять продажи акций через биржи и торговые площадки, которые не являются настоящими, то есть ссылка на данные площадки является ложной (фишинговой), но представляется как оригинальная, посредством этого разрабатываемые лица вступают в доверие к мошеннику и осуществляют инвестирование на фишинговом сайте, не думая о дальнейшей судьбе своих денежных средств, так как злоумышленники воссоздали положительную картину «богатства» и внушили это пострадавшему лицу. В дальнейшем, лицо, желающее вывести данные денежные средства сталкивается с тем, что эти средства не перечисляются обратно на банковский счет, так как их в натуральной форме нет, существует ли цифровая форма, которая ложно демонстрируется на фишинговом сайте инвестиций. Далее, мошенники блокируют номер телефона, через который осуществлялся звонок потерпевшему и исчезают из поля зрения пострадавшего и правоохранительных органов.

Особовыделяемой методикой совершения мошенничества, которая сохраняет анонимность злоумышленника – это использование технологии искусственного интеллекта. В последнее время развивается тенденция применения данной утилиты для обмана человека, путем установки программ дип-фейков, которые могут переделывать внешность человека и

его голос. Мошенники используют данную технологию при осуществлении видеозвонков, отправлении видео-сообщений в социальных сетях и при производстве телефонных звонков. Злоумышленники перед проведением данных действий тщательно узнают информацию об интересующим их человеке, путем использования методов социальной инженерии, телеграмм-ботов (ГлазБога и ШерлокБот, которые имеют функцию сбора всей информации о личности человека, путем анализа номера телефона разрабатываемого лица) и социальных сетей (в основном страницы в онлайн-мессенджерах открыты, тем самым злоумышленник может узнать информацию через друзей или близких родственников потерпевшего). Далее, после получения интересующей их информации, мошенники осуществляют видео- или аудио-звонки, представляясь представителем какой-либо компании или близким родственником, путем изменения своей внешности и голоса, тем самым потерпевшее лицо входит в доверие к злоумышленнику и выполняет его требования, вплоть до перевода денежных средств на его банковский счет.

Также необходимо выделить, что в 2025 году, законодатель выделил новые квалифицирующие признаки совершения преступления, предусмотренного статьей 187 «Неправомерный оборот средств платежа» Уголовного кодекса РФ. Введение произошло 24.06.2025 года, разработанная норма дефиниции была законодательно закреплена в Федеральном законе от 24.06.2025 года №176-ФЗ «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации» [3]. В данном федеральном законе законодатель выделил новый квалифицирующий признак для данного состава преступления, так как преступники разработали новые способы легализации денежных средств, путем использования банковских карт, которые активно покупались у других лиц из числа мирного населения или же обманным путем заполучали реквизиты данных носителей денежных средств для осуществления отмывания средств платежей. Данный состав преступлений, согласно следственно-судебной практике получил свою неофициальную аббревиатуру «Дропперство». Как отмечается в информационных и научных материалах, основными способами совершения IT-мошенничества являются перевод денежных средств на расчетные счета «дропперов» (лица, которые используют чужие банковские карты для легализации денежных средств, полученных преступным путем, например, в ходе мошеннических действий, в крупном размере, для сохранения своей анонимности), либо передача денежных средств через специально-

нанятых лиц – «курьеров». Использование данной преступной схемы позволяет мошенникам сохранять свою анонимность и минимизировать риски уголовного преследования сотрудниками правоохранительных органов.

Подводя итоги изученного параграфа, необходимо отметить, что способы и методы совершения мошенничества, путем использования информационно-телекоммуникационных технологий представляет из себя многогранно-сложную систему, включающая в себя меры психологического воздействия и технические способы вмешательства в функционирование цифровых систем мирного населения государства. Доминирующее положение в системе способов и методов совершения мошенничества занимает меры социальной инженерии, применяемые злоумышленниками. Реализация данных мер происходит посредством совершения телефонных звонков и рассылки сообщений через электронные почты и СМС. Эволюция способов и методов совершения данной категории преступления зависит от следующих факторов: анонимности, конспирации, возможность охвата большей аудитории (потерпевших) и активное использование преступниками технологий искусственного интеллекта.

Список литературы:

- [1] Аминов, И. Р. Криптовалюта как предмет преступлений коррупционной направленности / И. Р. Аминов, С. В. Трусов // Международный научный вестник. – 2025. – № 1. – С. 93-97. – DOI 10.24412/2782-3849-2025-1-93-97. – EDN MFDHNE;
- [2] Аминов, И. Р. Криминологический анализ мошенничества с использованием электронных средств платежа / И. Р. Аминов, И. В. Голубев // Право и управление. – 2026. – № 1. – С. 524-527. – DOI 10.24412/2224-9133-2026-1-524-527. – EDN JAPFON;
- [3] О внесении изменений в статью 187 Уголовного кодекса Российской Федерации : Федеральный закон от 24.06.2025 года № 176-ФЗ // Официальный интернет-портал правовой информации [Электронный ресурс]. – Режим доступа: <http://www.pravo.gov.ru> (дата обращения: 30.03.2026);
- [4] Димидов Д. С. Борьба с мошенничеством, совершенным с использованием информационно-коммуникационных технологий: проблемы и пути решений // Право и государство: теория и практика. 2024. № 12 (240). URL: <https://cyberleninka.ru/article/n/borba-s-moshennichestvom-sovershennym-s-ispolzovaniem-informatsionno-kommunikatsionnyh-tehnologiy-problemy-i-putiresheniy> (дата обращения: 30.03.2026).

References:

[1] Aminov, I.R. Cryptocurrency as the subject of corruption-related crimes/I.R. Aminov, S.V. Trusov//International Scientific Bulletin. – 2025. – № 1. – S. 93-97. – DOI 10.24412/2782-3849-2025-1-93-97. – EDN MFDHHE;

[2] Aminov, I. R. Criminological analysis of fraud using electronic means of payment/I. R. Aminov, I. V. Golubev//Law and Management. – 2026. – № 1. – S. 524-527. – DOI 10.24412/2224-9133-2026-1-524-527. – EDN JAPFON;

[3] On amendments to Article 187 of the Criminal Code of the Russian Federation: Federal

Law of 24.06.2025 No. 176-FZ//Official Internet Portal of Legal Information [Electronic Resource]. – Access mode: <http://www.pravo.gov.ru> (access date: 30.03.2026);

[4] Dimidov D. S. Combating fraud committed using information and communication technologies: problems and solutions//Law and state: theory and practice. 2024. №12 (240). URL: <https://cyberleninka.ru/article/n/borba-s-moshennichestvom-sovershennym-s-ispolzovaniem-informatsionno-kommunikatsionnyh-tehnologiy-problemy-i-puti-resheniy> (дата обращения: 30.03.2026).



**ЮРИДИЧЕСКОЕ ИЗДАТЕЛЬСТВО
«ЮРКОМПАНИ»**

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.

ЮРКОМПАНИ

www.law-books.ru