

DOI: 10.17803/1729-5920.2026.231.2.055-066

Е. И. Галяшина

Я. В. Комиссарова

Московский государственный юридический  
университет имени О.Е. Кутафина (МГЮА)

г. Москва, Российская Федерация

## Криминалистические подходы к противодействию преступлениям, совершаемым с использованием информационно-коммуникационных технологий

**Резюме.** В статье рассматриваются возможности криминалистики как юридической науки прикладного характера для совершенствования механизма противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий. Ключевая проблема состоит в том, что компьютерно опосредованная коммуникация преступника и жертвы осуществляется дистанционно, преступная деятельность (как подготовка, так и совершение правонарушения) тщательно маскируется, ее следы нивелируются за счет применения современных технологий. В связи с этим у сотрудников правоохранительных органов возникают сложности с установлением местонахождения преступника, его личности и иных обстоятельств, имеющих значение для раскрытия, расследования и предупреждения преступлений. Наряду с принятием на государственном уровне масштабных технических и правовых решений авторы полагают необходимым сосредоточить усилия криминалистов на многоаспектном анализе коммуникативной составляющей механизма преступлений, совершаемых с использованием информационно-коммуникационных технологий. Установлено, что медианарратив «жертвой мошенников может стать каждый» контрпродуктивен, так как он деморализует граждан, осложняя выявление и расследование рассматриваемой категории преступлений. Указано на целесообразность изменения подходов к изучению личности жертв мошенников (физических лиц) и формированию частных методик расследования отдельных видов преступлений в условиях цифровой трансформации общества.

**Ключевые слова:** цифровизация; информационно-коммуникационные технологии; противодействие преступлениям; криминалистика; коммуникация; криминалистическое изучение личности; механизм преступления; мошенничество; медианарратив; криминалистическая профилактика

**Для цитирования:** Галяшина Е. И., Комиссарова Я. В. Криминалистические подходы к противодействию преступлениям, совершаемым с использованием информационно-коммуникационных технологий. *Lex russica*. 2026. Т. 79. № 2. С. 55–66. DOI: 10.17803/1729-5920.2026.231.2.055-066

**Благодарности.** Исследование выполнено в рамках программы стратегического академического лидерства «Приоритет-2030» (центр компетенций «Социоправо»).

## Forensic Approaches to Investigating and Countering Crimes Facilitated by Information and Communication Technologies

Elena I. Galyashina

Yaroslava V. Komissarova

Kutafin Moscow State Law University (MSAL)

Moscow, Russian Federation

**Abstract.** The paper examines the potential of criminalistic science, understood as an applied legal discipline, to enhance mechanisms for combating crimes carried out using information and communication technologies (ICT). The key problems identified are: that ICT-mediated offender–victim communications occur remotely, that both the preparation and commission of offenses are carefully concealed, and that crime traces are often obscured by modern technologies. These factors create substantial difficulties for law enforcement in establishing offenders' locations, identities, and other circumstances essential to detection, investigation, and prevention. While large-scale technical and legal measures at the state level are necessary, the authors argue that criminalists should also prioritize a multidimensional analysis of the communicative component of ICT-enabled crimes. The study finds that the prevailing media narrative that «anyone can become a victim of fraud» is counterproductive: it demoralizes citizens and hampers the identification and investigation of such offences. The paper recommends revising approaches to studying victims' identities and developing targeted, specialized investigative methods for particular categories of ICT-enabled crimes in the context of digital transformation.

**Keywords:** digitalization; information and communication technologies; countering crime; forensics; communication; forensic personality studies; crime mechanism; fraud; medianarrative; forensic prevention

**Cite as:** Galyashina EI, Komissarova YaV. Forensic Approaches to Investigating and Countering Crimes Facilitated by Information and Communication Technologies. *Lex russica*. 2026;79(2):55-66. (In Russ.). DOI: 10.17803/1729-5920.2026.231.2.055-066

**Acknowledgements.** The study was carried out within the framework of the Priority-2030 Strategic Academic Leadership Program («Sociopravo» Competence Center).

### Введение

В условиях цифровой трансформации общества стремительное распространение информационно-коммуникационных технологий (ИКТ) оказывает значительное влияние на все сферы деятельности отдельно взятой личности и государства в целом, создавая одновременно преимущества и угрозы для их существования и развития. Злоумышленники, осваивая ИКТ опережающими темпами, всё чаще проявляют преступную активность в информационно-коммуникационной среде. Структура преступной деятельности при этом видоизменяется, непрерывно возникают новые способы совершения противоправных посягательств, их модернизация происходит в ускоренном темпе, что осложняет деятельность правоохранительных органов. Отлаженная годами система подготовки кадров и бюджетного финансирования подразделений, выполняющих разного рода функции

по противодействию преступности, не позволяет оперативно реагировать на новые вызовы.

Так, в криминальные схемы телефонного мошенничества на стороне преступников сегодня вовлечено большое количество молодежи, хорошо владеющей компьютерными технологиями, в то время как потерпевшими становятся преимущественно лица из социально незащищенных слоев населения с низким уровнем цифровой грамотности. Несмотря на некоторое уменьшение количества звонков с так называемых подменных номеров, данная практика еще не изжита. Злоумышленники продолжают использовать беспроводные средства мобильной связи, сим-боксы, возможности SIP-телефонии, виртуальных автоматических телефонных станций, фишинговые сайты или ссылки, ботнеты, фейковые биржевые площадки, криптообменники, «теневые» маркетплейсы и т.п.<sup>1</sup> С целью имитации подлинных речевых, голосовых и визуальных сообщений в мессенджерах и соци-

<sup>1</sup> URL: <https://мвд.рф/news/item/51089163/> (дата обращения: 15.03.2025).

альных сетях распространяются синтезированные с помощью искусственного интеллекта (ИИ) тексты, аудио- и/или видеофайлы. Важно, что для организации хищения денежных средств граждан России транснациональными организованными преступными группами используются кол-центры, действующие на территории недружественных государств, что затрудняет пресечение их деятельности.

Существенный рост и массовый характер мошенничества и иных преступных посягательств с использованием ИКТ потребовали от государства принятия беспрецедентных мер по борьбе с данным родом противоправными деяниями<sup>2</sup>. Создание механизма эффективного противодействия преступлениям, совершаемым с применением ИКТ, а также уменьшение причиняемого таким образом ущерба признаны одной из приоритетных национальных целей развития Российской Федерации на ближайшие годы<sup>3</sup>.

Президент РФ В. В. Путин 5 марта 2025 г. провел по видеосвязи совещание с членами Правительства, в ходе которого рассматривались вопросы профилактики общественно опасных деяний, совершаемых с использованием ИКТ, прежде всего телефонного и интернет-мошенничества<sup>4</sup>. Отмечалось, что, несмотря на законодательные и организационные меры, принимаемые органами государственной власти и управления, необходимый уровень безопасности в информационно-коммуникационной сфере пока не достигнут. Это отчасти объясняется виктимным поведением жертв мошенников, низким уровнем их правовой и цифровой грамотности наряду с применением преступниками высокотехнологичных способов анонимизации, методов социальной инженерии (манипулятивных технологий) при общении с потенциальными потерпевшими.

Общественно опасные деяния, совершаемые с использованием ИКТ, чрезвычайно разнообразны. По данным специалистов в области уголовного права, в УК РФ содержится 35 составов преступлений, объективная сторона которых охватывает применение ИКТ: из них 8 закрепляют рассматриваемый признак в качестве криминообразующего, 23 — квалифицирующего и 4 — особо квалифицирующего<sup>5</sup>.

Проблема выявления, раскрытия и расследования такого рода преступлений выходит далеко за пределы предметной области криминалистики и компетенции правоохранительных органов. Поэтому в ходе совещания, проведенного Президентом РФ, председатель Следственного комитета РФ А. И. Бастрыкин предложил рассмотреть вопрос о создании Агентства по противодействию телефонному, интернет-мошенничеству и другим видам интернет-преступлений.

Разумеется, это не означает, что криминалистика не может предложить действенные меры, достаточно результативные не только в текущей ситуации, но и в перспективе. Так, согласно вышеупомянутой Концепции государственной системы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий (далее — Концепция), в целях повышения эффективности расследования соответствующей категории уголовных дел информационно-аналитическое обеспечение функционирования указанной системы может включать разработку единого методического подхода (криминалистической методики) расследования данных преступлений, аккумулирующего накопленный в разных странах мира положительный опыт.

Рассмотрим некоторые прикладные аспекты научного моделирования указанной частной криминалистической методики.

<sup>2</sup> Распоряжение Правительства РФ от 30.12.2024 № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» // URL: <http://publication.pravo.gov.ru/document/0001202501090003> (дата обращения: 14.03.2025).

<sup>3</sup> Единый план по достижению национальных целей развития до 2030 года и на перспективу до 2036 года // URL: <http://static.government.ru/media/files/ZsnFICpxWknEXeTfQdmcFHNei2FhcROA.pdf> (дата обращения: 14.03.2025).

<sup>4</sup> Совещание с членами Правительства // URL: <http://www.kremlin.ru/events/president/news/76409> (дата обращения: 14.03.2025).

<sup>5</sup> Скрипченко Н. Ю. Использование информационно-телекоммуникационных сетей в криминальных целях: нормативный учет и перспективы расширения уголовно-правового значения // RUDN Journal of Law. 2024. Т. 28. № 1. С. 200.

## Общая характеристика ИКТ

В Концепции под ИКТ понимаются «процессы и методы создания, обработки, распространения информации, а также способы и средства их осуществления», информационно-коммуникационная сфера описывается как «совокупность информационно-телекоммуникационных сетей, включая сеть “Интернет”, технологической инфраструктуры, обеспечивающей их функционирование, и различных форм человеческой активности, осуществляемой посредством их использования».

В Федеральном законе «Об информации, информационных технологиях и о защите информации»<sup>6</sup> понятие ИКТ отсутствует. При этом в ст. 2 понятие «информация» определено как «сведения (сообщения, данные) независимо от формы их представления»; под информационными технологиями подразумеваются «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов»; информационно-телекоммуникационная сеть рассматривается как «технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники». Если информация была передана или получена пользователем такой сети, то она именуется электронным сообщением. Иными словами, любые текстовые, аудио-, видеоданные, транслируемые по линиям связи с использованием средств вычислительной техники, являются электронными сообщениями.

Несмотря на сходство дефиниций понятий «информационно-коммуникационные технологии» в Концепции и «информационные технологии» в Федеральном законе «Об информации, информационных технологиях и о защите информации», ключевое различие со

всей очевидностью детерминировано семантикой слова «коммуникационные», определяющей процессы и методы не только информационного обмена, но и создания информации, ее направленность на достижение поставленных целей, а также отражающей коммуникативную составляющую человеческого общения.

Термин «коммуникация» появился в научной литературе в начале XX в. Сегодня им обозначают всё многообразие информационных процессов между неодушевленными объектами, людьми, с представителями животного мира. Понятия «общение» и «коммуникация» пересекаются, когда рассматриваются передача информации от человека к человеку (межличностная коммуникация) и обмен информацией в обществе (социальная коммуникация)<sup>7</sup>.

Обмен информацией осуществляется посредством сигналов. Сигнал — это знак, несущий сообщение о каком-либо событии или явлении, состоянии объекта наблюдения. Используя совокупность сигналов, можно охарактеризовать любое сколь угодно сложное событие<sup>8</sup>. Такой подход позволяет описать всё многообразие источников криминалистически значимой информации, включая те, что появляются с течением времени (когда на определенном историческом этапе их возникновение не прогнозируется). Это обусловило необходимость выделения в современных учебниках по криминалистике самостоятельной группы следов — знаковых<sup>9</sup>.

Понятие «коммуникационные технологии» широко применяется в профессиональном дискурсе специалистов в сфере рекламы и связей с общественностью, которые понимают их как совокупность приемов, процедур, средств и методов, используемых в процессе коммуникационного воздействия субъектом коммуникации с целью достижения поставленных целей и задач в разных областях человеческой деятельности<sup>10</sup>.

<sup>6</sup> Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2025) // СПС «Консультант-Плюс».

<sup>7</sup> Комиссарова Я. В. Проблемные аспекты коммуникативной составляющей судопроизводства // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 10 (110). С. 39.

<sup>8</sup> Морковкин В. В., Богачёва Г. Ф., Луцкая Н. М. Большой универсальный словарь русского языка : около 30 000 наиболее употребительных слов / под ред. проф. В. В. Морковкина. М. : АСТ-Пресс школа, 2018.

<sup>9</sup> См., например: Криминалистика : учебник / под ред. А. И. Бастрыкина, Е. П. Ищенко, Я. В. Комиссаровой. 2-е изд., перераб. и доп. М. : Проспект, 2024. С. 42–43.

<sup>10</sup> См., например: Савченко Е. А., Макарова Т. П. PR и PR-технологии: сущность, цели, задачи, функции // Образование. Наука. Научные кадры. 2019. № 3. С. 178–180.

Термин «информационно-коммуникационные технологии» обозначает различного рода и назначения технические средства (в широком смысле слова), а также технологии, которые обеспечивают связь, обмен данными и глобальную коммуникацию. При этом наряду с передовыми (такими, как искусственный интеллект, робототехника, 5G/6G, Web3, квантовые вычисления и др.) понятие ИКТ охватывает и постепенно вытесняемые, но всё ещё применяемые для общения коммуникационные технологии с использованием стационарных телефонов, радио- и телевидения.

Очевидно, что «массовое использование ИКТ огромным количеством людей неизбежно приводит к их использованию в криминальных целях»<sup>11</sup>, а необходимость применения при противодействии преступности не только открывает новые возможности, но и одновременно создает труднопрогнозируемые риски для уголовного судопроизводства<sup>12</sup>.

### ИКТ как элемент механизма преступления

По данным МВД России, количество преступлений, совершенных с использованием ИКТ, в 2023 г. по сравнению с 2022 г. увеличилось на 30 %, в 2024 г. их прирост по отношению к 2023 г. составил 13,1 %, а доля превысила 40 % от числа всех зарегистрированных преступлений, в то время как раскрываемость колеблется на уровне 30–35 %<sup>13</sup>. ИКТ открывают новые возможности для преступников, способствуют увеличению масштабов преступной деятельности, которая становится всё более изощренной.

К числу ИКТ, позволяющих совершать преступления и скрывать их следы, относятся средства анонимизации, спуфинга, смены фактиче-

ского IP-адреса, подменные номера телефонов, фиктивные данные для регистрации на интернет-платформах, временные сим-карты, подставные счета, оформленные на третьих лиц, так называемые виртуальные кошельки и многое другое<sup>14</sup>.

Для сокрытия связи между пользователем сети Интернет и конкретной реальной личностью могут создаваться вымышленная виртуальная личность или незаконно использоваться чужие персональные данные, т.е. злоумышленник будет осуществлять противоправную деятельность от лица ничего об этом не подозревающего человека. Для этого создается фейковый аккаунт в социальной сети и применяются методы социальной инженерии.

Возможности взаимодействия с жертвой в условиях, обеспечивающих анонимность злоумышленника, повышают социальную опасность преступлений с использованием ИКТ. Как справедливо отмечает Ю. В. Гаврилин, следствием цифровой трансформации общества неизбежно является развитие дистанционных способов совершения преступлений, исключающих непосредственный контакт соучастников как между собой, так и с потерпевшими. Субъекты преступления взаимодействуют с потерпевшими или третьими лицами опосредованно, с использованием средств связи и информационных ресурсов сети Интернет. Применяя методы социальной инженерии для хищения денежных средств, направленные на введение потерпевшего в заблуждение относительно истинной цели телефонного вызова, злоумышленники активно используют технологии ИИ, включая синтез голоса и речи, видеоизображений<sup>15</sup>. Это позволяет мошенникам манипулировать поведением человека, подчинять его своей воле вплоть до склонения к преступным действиям.

<sup>11</sup> Мещеряков В. А. Теоретические основы слеодообразования в цифровой криминалистике : монография. М. : Проспект, 2022. С. 55.

<sup>12</sup> См., например: Чурикова А. Ю. Использование информационных технологий и систем в уголовном судопроизводстве: возможности, риски, правовое регулирование : автореф. дис. ... д-ра юрид. наук. Саратов, 2024.

<sup>13</sup> URL: <https://habr.com/ru/news/877022/> (дата обращения: 14.03.2025).

<sup>14</sup> Антонян Е. А., Бархатова Е. В. Противодействие киберпреступности // Евразийский Союз Ученых. 2019. № 7 (64). С. 54–57.

<sup>15</sup> Гаврилин Ю. В. Тенденции цифровой трансформации преступности и факторы, ее обуславливающие // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы : сборник статей Международной научно-практической конференции, Москва, 23 октября 2020 г. / под общ. ред. И. Г. Чистобородова, А. Л. Ситковского, В. О. Лапина. М. : Академия управления МВД России, 2020. С. 204–212.

С учетом изложенного при формировании статистической отчетности в перечень преступлений, совершенных с применением ИКТ или в сфере компьютерной информации, отмечаемых по способу совершения преступления, была включена технология Deepfake (методика синтеза аудио- или визуальной информации, основанная на ИИ, с целью создания сравнимой с оригиналом копии аудио- или видеоизображения)<sup>16</sup>. Однако этого мало. Сегодня остро стоит вопрос о разработке методического обеспечения криминалистического анализа следовой картины коммуникации мошенника с жертвой с целью распознавания криминального сценария речевого общения, обнаружения признаков подделки голосовых, видео- или текстовых сообщений, изготовленных с помощью ИИ и используемых в целях как повышения уровня доверия потерпевшего к собеседнику, так и порождения страха распространения дискредитирующей информации, содержащейся в цифровой подделке<sup>17</sup>. В ситуации, когда следователь нуждается в специальных знаниях для установления факта манипулятивного психологического воздействия на потерпевшего и выявления фальсификации текстового сообщения, изображения, звуко- и видеозаписей, криминалистика может дать научно обоснованные рекомендации по фиксации, изъятию и криминалистическому исследованию вербально-визуальных следов применения мошеннических схем.

Данные статистики позволяют спрогнозировать дальнейшее увеличение количества зарегистрированных преступлений, совершаемых

с использованием ИКТ<sup>18</sup>. Речь идет не только о стремлении преступников нажать за счет жертв. Информационно-коммуникационная сфера выступает благоприятной площадкой для вредоносной пропаганды, а также посягательств на традиционные ценности общества и смысловые ориентиры личности<sup>19</sup>. Применение ИКТ в преступных целях может оказывать значительное влияние на масштабы, скорость совершения и объем уголовно наказуемых деяний, включая те, что связаны с терроризмом и экстремизмом. Инструментарий ИКТ с использованием ИИ модифицирует механизм преступления, превращая преступную деятельность из угрозы общественной безопасности в экзистенциальный вызов для всех систем национальной безопасности каждого отдельно взятого государства и, более того, в международном масштабе.

Ряд мер, которые необходимо принять государствам для предотвращения киберпреступности и борьбы с ней, были сформулированы в Конвенции Организации Объединенных Наций против киберпреступности, принятой Генеральной Ассамблеей в декабре 2024 г. Конвенция, будучи первым всеобъемлющим международным договором по этому вопросу, направлена на укрепление международного сотрудничества при обмене электронными доказательствами по делам о тяжких преступлениях<sup>20</sup>.

В Конвенции используется семантически сходный с ИКТ термин «информационно-коммуникационная система», который означает любое устройство или группу соединенных или взаимосвязанных устройств, одно или

<sup>16</sup> Указание Генпрокуратуры России № 11/11, МВД России № 1 от 17.01.2023 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности. Перечень № 25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации» // URL: <https://sudact.ru/law/ukazanie-genprokuratury-Rossii-n-1111-mvd-Rossii/> (дата обращения: 14.03.2025).

<sup>17</sup> *Галяшина Е. И., Антонян Е. А., Богатырев К. М.* Защита от злоупотребления искусственным интеллектом и нейротехнологиями в аспекте медиабезопасности : монография / отв. ред. Е. И. Галяшина. М. : Проспект, 2025. С. 60–61.

<sup>18</sup> *Квасникова Т. В.* Новые направления мошеннических посягательств с использованием цифровых технологий // Таможенная политика России на Дальнем Востоке. 2024. № 2 (107). С. 81–86.

<sup>19</sup> *Галяшина Е. И.* О понятии цифровой трансформации в криминалистике // Всероссийский криминологический журнал. 2024. Т. 18. № 4. С. 379–389.

<sup>20</sup> Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям. Принята резолюцией Генеральной Ассамблеи от 24.12.2024 79/243 // URL: <https://documents.un.org/doc/undoc/gen/n24/426/76/pdf/n2442676.pdf> (дата обращения: 14.03.2025).

несколько из которых по команде программы производят сбор, хранение и автоматическую обработку электронных данных; под «электронными данными» подразумевается любое представление фактов, информации или концепций в форме, пригодной для обработки в информационно-коммуникационной системе, включая соответствующую программу, в результате действия которой информационно-коммуникационная система выполняет ту или иную функцию (ст. 2 Конвенции).

Прогрессирующая зависимость социума от ИКТ определяет дальнейшую экспансию криминала в виртуальное пространство. В этой связи мы солидарны с теми учеными, кто предлагает на уровне УК РФ использование ИКТ включить в числоотягающих обстоятельств. Как обоснованно пишет Е. А. Русскевич, существенные трудности в процессе раскрытия и расследования преступлений, возникающие в связи с неправомерным сокрытием либо изменением идентификаторов ИКТ, обеспечивают требуемый для отягчающего обстоятельства значимый перепад в уровне общественной опасности деяния<sup>21</sup>.

Изложенное предложение нашло поддержку у правоприменителей: в ходе совещания с Президентом страны председатель СК России А. И. Бастрыкин высказался за то, чтобы использование современных информационных технологий и искусственного интеллекта в противоправных целях стало отягчающим обстоятельством при квалификации деяния.

### О значении криминалистического изучения личности

Криминалистика находится на переднем крае борьбы с преступностью, успешность которой во многом зависит от качества аналитической работы следователей и дознавателей по уяс-

нению механизма преступной деятельности в целях установления обстоятельств, подлежащих доказыванию.

Стремление получить желаемое мотивирует злоумышленника. Руководствуясь поставленными целями, он выбирает способ совершения преступления. Реализуя преступный замысел, субъект действует в конкретной обстановке: взаимодействуя со средой, он вносит в нее изменения (оставляет следы), анализируя которые правоприменители получают информацию о событии преступления, позволяющую установить и изобличить преступника. Поэтому учение о криминалистических методах и средствах изучения личности занимает важное место среди частных криминалистических теорий<sup>22</sup>.

Суть любой мошеннической схемы (когда речь идет о физических лицах) — завоевание доверия человека с целью его дальнейшего обмана. Поэтому очевидна необходимость не только повышения цифровой грамотности, но и формирования у граждан определенной культуры коммуникации на основе принципа «нулевого доверия» (концепция, известная как Zero Trust, — «незнакомцу не доверяй без проверки»). В этой связи представляется важным углубленный криминалистический анализ дел о мошенничестве в отношении физических лиц (по видам преступлений) для составления портрета жертвы подобных преступлений за счет выявления криминалистически значимых признаков.

Не следует ограничиваться использованием результатов исследований в данной области, проводимых психологами и криминологами<sup>23</sup>. Их подходы к составлению виктимологического портрета жертвы преступления отличаются от тех, что применяются в процессе криминалистического портретирования. Описания индивидуально-психологических особенностей жертв мошенников, их деления на «доверчивых» и

<sup>21</sup> Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения. М. : Инфра-М, 2019. С. 126–127.

<sup>22</sup> См., например: Криминалистика / Т. В. Аверьянова, Р. С. Белкин, И. А. Возгрин [и др.] ; под ред. Р. С. Белкина, В. Г. Коломацкого, И. М. Лузгина. М. : Акад. МВД России, 1995. Т. 1 : История, общая и частные теории. С. 221–233 ; Криминалистическое изучение личности : науч.-практ. пособие для магистров / А. Г. Бедрезов, Т. С. Волчецкая, Н. В. Галяшин [и др.] ; отв. ред. Я. В. Комиссарова. М. : Проспект, 2016 ; Криминалистика / под ред. д-ра юрид. наук, проф. И. М. Комарова. М. : Юрлитинформ, 2023. С. 402–419.

<sup>23</sup> См., например: Доув М. Психология мошенничества. Методы убеждения и мошенничества / пер. с англ. Е. М. Тарабановой. М. : Гуманитарный центр, 2022. С. 119–143 ; Кабанов П. А. Жертвы кибермошенничества как один из объектов современной кибервиктимологии: краткий статистический анализ показателей криминальной виктимности 2021–2022 гг. // Виктимология. 2023. Т. 10. № 1. С. 17–28.

«алчных»<sup>24</sup> явно недостаточно для принятия мер криминалистической профилактики, особенно с учетом данных психологов о том, что ключевой характеристикой жертвы телефонного мошенничества является не стремление к обогащению, а страх потерять имеющееся<sup>25</sup>.

На наш взгляд, при совершении мошенничества в отношении физических лиц в группе риска преимущественно находятся:

1) страдающие психическими расстройствами (речь идет о множестве специфических психических состояний, когда проблемы могут не осознаваться как самим человеком, так и его близким окружением);

2) совершающие правонарушения в целях незаконного обогащения, в том числе уклоняющиеся от уплаты налогов, сборов, страховых взносов;

3) лица, подпадающие под категорию, обозначенную «антигероями» Базилио и Алисой в детском художественном фильме «Приключения Буратино»: «Покуда есть на свете дураки, обманом жить нам, стало быть, с руки» (диапазон широк — от девиантного поведения до так называемого наивного оптимизма, рассматриваемого психологами в качестве потенциально токсичной формы позитивного мышления)<sup>26</sup>.

Нетрудно заметить, что в приведенной классификации нет места размытой характеристике «пожилые лица», зато становится понятно, какими причинами могут обуславливаться опасения конкретного человека потерять имеющееся. Такой подход упрощает выработку мер криминалистической профилактики рассматриваемой категории преступлений.

Что касается первой группы, имеет смысл рассмотреть возможность автоинформирования граждан (например, путем СМС-оповещений, направляемых операторами сотовой связи, по аналогии с оповещениями об изменении метеоусловий) о том, что в случае совершения в отношении них мошеннических действий

рекомендуется обратиться за психиатрической помощью.

По данным специалистов, от 65 до 90 % больных с психическими расстройствами изначально обращаются к врачам общей практики, а не к психиатрам. До 70 % людей, совершивших попытку самоубийства, в течение трех месяцев перед этим обращались к терапевтам, невропатологам, кардиологам и другим врачам, 35 % из них длительно лечились у терапевтов или невропатологов<sup>27</sup>. В какой-то мере обратиться к психиатру людям мешают укоренившиеся негативные стереотипы. Возможно, в случае телефонного мошенничества эти обращения могли бы сыграть позитивную роль. СМИ пестрят рассказами о пожилых людях, передавших большие суммы «на сохранение» мошенникам, когда родственникам не было известно о наличии сбережений. Не секрет, что многие психические расстройства ведут к разрыву связей именно с близкими людьми, из-за чего редко диагностируются на ранней стадии.

Всемирная организация здравоохранения настоятельно призывает директивные органы и активистов разных стран взять на себя повышенные обязательства и активизировать меры по изменению установок, практики и подходов, имеющих отношение к психическому здоровью, его детерминантам и оказанию психиатрической помощи<sup>28</sup>. Не исключено, что системный анализ поведения людей, ставших жертвами мошенников, проводимый специалистами, может сыграть положительную роль с точки зрения обеспечения ранней диагностики некоторых распространенных психических расстройств.

Данный вопрос является крайне деликатным и нуждается в комплексной проработке. На наш взгляд, целесообразно сформировать рабочую группу из специалистов разного профиля для того, чтобы каждая формулировка и, возможно, правовые последствия принятых решений не выходили за границы этики.

<sup>24</sup> См., например: *Ревенко Н. И.* Криминалистическая характеристика мошенничества с использованием информационно-телекоммуникационных технологий // Вестник Омского университета. Серия «Право». 2024. Т. 21. № 2. С. 88.

<sup>25</sup> *Мешкова Н. В., Кудрявцев В. Т., Ениколопов С. Н.* К психологическому портрету жертв телефонного мошенничества // Вестник Московского университета. Серия 14 «Психология». 2022. № 1. С. 138–157.

<sup>26</sup> Подробно см.: *Психология глупости* / под ред. Ж.-Ф. Мармьона; пер. с фр. Э. Болдиной. М.: Эксмо, 2019.

<sup>27</sup> Психические расстройства в общемедицинской практике // URL: <https://lrkpnb.gosuslugi.ru/novosti/psihicheskie-rasstroystva-v-obshchemeditsinskoy-praktike.html> (дата обращения: 14.03.2025).

<sup>28</sup> ВОЗ: необходимо срочно изменить подход к психическому здоровью и оказанию психиатрической помощи // URL: <https://www.who.int/ru/news/item/17-06-2022-who-highlights-urgent-need-to-transform-mental-health-and-mental-health-care> (дата обращения: 14.03.2025).

В отношении лиц, включенных во вторую группу, целесообразно проработать вопрос об усилении уголовной ответственности за совершение преступления, если в отношении субъекта преступления были предприняты мошеннические действия, в силу которых мошенники завладели деньгами и ценностями, добытыми преступным путем. Когда незаконным способом нажитые средства переходят к мошенникам, они не могут быть изъяты для погашения причиненного ущерба или конфискации в пользу государства<sup>29</sup>.

Изменению позиции субъектами последней группы отчасти могло бы способствовать смещение акцентов в информационном поле.

Участники проведенной кафедрой криминалистики Университета имени О.Е. Кутафина (МГЮА) 10 февраля 2025 г. совместно с Молодежной секцией Международного союза криминалистов дизайн-сессии «Криминалистическая превенция телефонного мошенничества» обратили внимание на то, что стереотип, навязанный СМИ, «жертвой мошенников может стать каждый» сегодня является контрпродуктивным<sup>30</sup>. С одной стороны, можно согласиться с тем, что к любому человеку в силу его индивидуально-психологических особенностей и некоторых других факторов злоумышленники могут подобрать ключ — побудить выполнить их требования. С другой стороны, данный тезис деморализует граждан, превращая в безвольных жертв, что осложняет выявление и расследование рассматриваемой категории преступлений.

На наш взгляд, назрела необходимость смены медианарратива: следует отказаться от возведения телефонных мошенников в ранг мастеров гипноза и властителей душ и определить круг обязанностей, которые могут и должны нести граждане в условиях цифровой трансформации общества в целях предупреждения совершения преступлений с использованием ИКТ. В Концепции отмечены необходимость повышения уровня осведомленности граждан о методах совершения противоправных деяний и

способах защиты от них, значение социальной рекламы, направленной на воспитание цифровой грамотности, но ничего не сказано о личной ответственности граждан за свою информационную безопасность (в широком смысле слова) и сохранность имущества.

## Заключение

Современная криминалистика — не застывшая, а динамически развивающаяся на основе интеграции и дифференциации область научных знаний, нацеленная на разработку средств, приемов и методов обнаружения, фиксации, изъятия, исследования следов преступления и использования полученной таким образом информации в доказывании по уголовным делам. Появление новых видов преступлений, совершаемых с применением ИКТ, обусловило изменение следовой картины противоправных деяний, что никоим образом не меняет природу криминалистики как юридической науки. В настоящее время в условиях цифровизации общественной жизни наблюдается некоторое смещение фокуса внимания ученых и практиков на изучение закономерностей, связанных с техническими аспектами преступной деятельности. Однако это не должно мешать анализу ее коммуникативной составляющей.

Преступления как совершают, так и расследуют люди. На данном этапе развития общества и государства представляются утопическими идеи авторов научных публикаций, полагающих, что в обозримом будущем «раскрытие преступлений на основе баз данных о лице, накопленных в агрегированных системах данных государства-платформы, в сети Интернет, телекоммуникационных, информационных каналах связи, будет осуществляться, разумеется, не людьми-«киберследователями», а техническими интеллектуальными агентами»<sup>31</sup>.

Другое дело — изменение подходов к формированию и совершенствованию частных методик расследования отдельных видов пре-

<sup>29</sup> Наше предложение в определенной мере коррелирует с вышеобозначенной позицией СК России относительно необходимости усиления ответственности за преступления, совершаемые с применением ИКТ.

<sup>30</sup> Ученые-криминалисты обсудили превенцию телефонного мошенничества // URL: <https://msal.ru/news/prepodavately-universiteta-imeni-o-e-kutafina-mgyua-rasskazali-o-preventsii-telefonnogo-moshennicheska/> (дата обращения: 14.03.2025).

<sup>31</sup> Власова С. В. К вопросу о приспособлении уголовно-процессуального механизма к цифровой реальности // Библиотека криминалиста. Научный журнал. 2018. № 1. С. 14.

ступлений, обусловленное расширением сферы применения ИКТ.

В рамках XII Московского инновационного юридического форума 26 марта 2025 г. кафедра криминалистики Университета имени О.Е. Кутафина (МГЮА) провела панельную дискуссию «Криминалистическое обеспечение противодействия мошенничеству, совершаемому с использованием информационно-телекоммуникационных технологий»<sup>32</sup>. Предваряя выступления спикеров, модератор (соавтор статьи Я. В. Комиссарова) отметил, что за счет синергии правовых, уголовно-процессуальных и криминалистических подходов в современных условиях все преступления условно можно разделить на три группы:

а) преступления, методика расследования которых позволяет следователю самостоятельно получать криминалистически значимую информацию в установленном законом порядке (например, направленные против личности);

б) преступления, алгоритм расследования которых строится на привлечении в установленном законом порядке лиц, обладающих

специальными знаниями, предоставляющих следователю криминалистически значимую информацию для принятия процессуальных решений (например, в сфере компьютерной информации);

в) преступления, криминалистический алгоритм расследования которых может быть реализован в соответствии с действующим УПК РФ только после выработки и принятия на государственном уровне масштабных технических и правовых решений.

В последнюю группу входят преступления, совершаемые с использованием ИКТ. Вступление в силу федерального закона «О создании государственных информационных систем по противодействию правонарушениям (преступлениям), совершаемым с использованием информационно-телекоммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации»<sup>33</sup> задает новый вектор научных исследований, с учетом которого криминалистам предстоит модифицировать работу по формированию соответствующих частных методик расследования преступлений.

#### СПИСОК ЛИТЕРАТУРЫ

Антонян Е. А., Бархатова Е. В. Противодействие киберпреступности // Евразийский Союз Ученых. 2019. № 7 (64). С. 54–57.

Власова С. В. К вопросу о приспособлении уголовно-процессуального механизма к цифровой реальности // Библиотека криминалиста. Научный журнал. 2018. № 1. С. 9–18.

Гаврилин Ю. В. Тенденции цифровой трансформации преступности и факторы, ее обуславливающие // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы : сборник статей Международной научно-практической конференции, Москва, 23 октября 2020 г. / под общ. ред. И. Г. Чистобородова, А. Л. Ситковского, В. О. Лапина. М. : Академия управления МВД России, 2020. С. 204–212.

Галяшина Е. И. О понятии цифровой трансформации в криминалистике // Всероссийский криминологический журнал. 2024. Т. 18. № 4. С. 379–389.

Галяшина Е. И., Антонян Е. А., Богатырев К. М. Защита от злоупотребления искусственным интеллектом и нейротехнологиями в аспекте медиабезопасности : монография / отв. ред. Е. И. Галяшина. М. : Проспект, 2025. 272 с.

Доув М. Психология мошенничества. Методы убеждения и мошенничества / пер. с англ. Е. М. Тарабановой. М. : Гуманитарный центр, 2022. 224 с.

Кабанов П. А. Жертвы кибермошенничества как один из объектов современной кибервиктимологии: краткий статистический анализ показателей криминальной виктимности 2021–2022 гг. // Виктимология. 2023. Т. 10. № 1. С. 17–28.

Квасникова Т. В. Новые направления мошеннических посягательств с использованием цифровых технологий // Таможенная политика России на Дальнем Востоке. 2024. № 2 (107). С. 81–86.

<sup>32</sup> Криминалисты vs мошенники, использующие информационно-телекоммуникационные технологии // URL: <https://msal.ru/news/kriminalisty-vs-moshenniki-ispolzuyushchie-informatsionno-telekommunikatsionnye-tekhnologii/> (дата обращения: 01.04.2025).

<sup>33</sup> URL: <https://sozd.duma.gov.ru/bill/842276-8> (дата обращения: 01.04.2025).

Комиссарова Я. В. Проблемные аспекты коммуникативной составляющей судопроизводства // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 10 (110). С. 38–46.

Криминалистика / под ред. д-ра юрид. наук, проф. И. М. Комарова. М. : Юрлитинформ, 2023. 712 с.

Криминалистика. Т. 1 : История, общая и частные теории / Т. В. Аверьянова, Р. С. Белкин, И. А. Возгрин [и др.] ; под ред. Р. С. Белкина, В. Г. Коломацкого, И. М. Лузгина. М. : Акад. МВД России, 1995. 278 с.

Криминалистика : учебник / под ред. А. И. Бастрыкина, Е. П. Ищенко, Я. В. Комиссаровой. 2-е изд., перераб. и доп. М. : Проспект, 2024. 544 с.

Криминалистическое изучение личности : науч.-практ. пособие для магистров / А. Г. Бедризов, Т. С. Волчецкая, Н. В. Галяшин [и др.] ; отв. ред. Я. В. Комиссарова. М. : Проспект, 2016. 224 с.

Мешкова Н. В., Кудрявцев В. Т., Ениколопов С. Н. К психологическому портрету жертв телефонного мошенничества // Вестник Московского университета. Серия 14 «Психология». 2022. № 1. С. 138–157.

Мещеряков В. А. Теоретические основы следообразования в цифровой криминалистике : монография. М. : Проспект, 2022. 176 с.

Психология глупости / под ред. Ж.-Ф. Мармьона ; пер. с фр. Э. Болдиной. М. : Эксмо, 2019. 320 с.

Ревенко Н. И. Криминалистическая характеристика мошенничества с использованием информационно-телекоммуникационных технологий // Вестник Омского университета. Серия «Право». 2024. Т. 21. № 2. С. 87–90.

Рускевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения. М. : Инфра-М, 2019. 227 с.

Савченко Е. А., Макарова Т. П. PR и PR-технологии: сущность, цели, задачи, функции // Образование. Наука. Научные кадры. 2019. № 3. С. 178–180.

Скрипченко Н. Ю. Использование информационно-телекоммуникационных сетей в криминальных целях: нормативный учет и перспективы расширения уголовно-правового значения // RUDN Journal of Law. 2024. Т. 28. № 1. С. 196–214.

Чурикова А. Ю. Использование информационных технологий и систем в уголовном судопроизводстве: возможности, риски, правовое регулирование : автореф. дис. ... д-ра юрид. наук. Саратов, 2024. 48 с.

## REFERENCES

Antonyan EA, Barkhatova EV. Countering cybercrime. *Eurasian Union of Scientists (EUS)*. 2019;7(64):54-57. (In Russ.).

Averyanova TV, Belkin RS, Vozgrin IA, et al. Belkin RS, Kolomatsky VG, Luzgin IM (eds.). *Forensics*. Vol. 1: History, general and specific theories. Moscow: MIF RF Academy Publ.; 1995. (In Russ.).

Bastrykin AI, Ishchenko IP, Komissarova YaV (eds.). *Criminalistics*. 2nd ed. Moscow: Prospekt Publ.; 2024. (In Russ.).

Bedrizov AG, Volchetskaya TS, Galyashin NV, et al. Komissarova YaV (ed.). *Forensic study of personality*. Moscow: Prospekt Publ.; 2016. (In Russ.).

Churikova AYU. Use of information technologies and systems in criminal proceedings: opportunities, risks, legal regulation. *Dr. Sci. (Law) Diss. Author's Abstract*. Saratov; 2024. (In Russ.).

Douv M. Psychology of fraud. Methods of persuasion and fraud. Tr. from English by Tarabanova EM. Moscow: Gumanitarnyi tsentr Publ.; 2022. (In Russ.).

Galyashina EI (ed.), Antonyan EA, Bogatyrev KM. Protection against artificial intelligence and neurotechnology abuse in terms of media security. Moscow: Prospekt Publ.; 2025. (In Russ.).

Galyashina EI. On the Concept of Digital Transformation in Criminalistics. *Russian Journal of Criminology*. 2024;18(4):379-389. (In Russ.).

Gavrilin YuV. Trends in the digital transformation of crime and the factors driving it. In: Chistoborodov IG, Sitkovskogo AL, Lapina VO (eds). *Strategic development of the system of the Ministry of Internal Affairs of Russia: State, trends, prospects*. Collection of articles of the International Scientific and Practical Conference, Moscow, October 23, 2020. Moscow: MIA Academy of Management Publ.; 2020. (In Russ.).

Kabanov PA. Victims of cyber theft as an object of modern Russian cybervictimology: a criminological analysis of statistical indicators of criminal victimhood 2021–2022. *Viktimologiya [Victimology]*. 2024;11(1):25-42. (In Russ.). DOI: 10.47475/2411-0590-2024-11-1-25-42.

Komarov IM. *Criminalistics*. Moscow: Yurлитинформ Publ.; 2023. (In Russ.).

- Komissarova YaV. Problematic Aspects of the Communicative Component of Legal Proceedings. *Courier of Kutafin Moscow State Law University (MSAL)*. 2023;10(110):38-46. (In Russ.).
- Kvasnikova TV. New Areas of Fraudulent Attacks Committed through Digital Technologies. *Customs Policy of Russia in the Far East*. 2024;2(107):81-86. (In Russ.).
- Marmontel JF. Psychology of stupidity. Moscow: Eksmo Publ.; 2019. (In Russ.).
- Meshcheryakov VA. Theoretical foundations of trace formation in digital forensics. Moscow: Prospekt Publ.; 2022.
- Meshkova NV, Kudryavtsev VT, Enikolopov SN. To the Psychological Portrait of the Victims of Telephone Fraud. *Vestnik Moskovskogo Universiteta. Seriya 14. Psikhologiya [Moscow University Psychology Bulletin]*. 2021;1:138-157. (In Russ.). DOI: 10.11621/vsp.2022.01.06.
- Revenko NI. Criminalistic Characteristics of Frauds Committed Using Information and Telecommunication Technologies. *Vestnik Omskogo universiteta. Seriya «Pravo» [Herald of Omsk University. Series «Law»]*. 2024;21(2):87-90. (In Russ.). DOI: 10.24147/1990-5173.
- Ruskevich EA. Criminal law and «digital crime»: problems and solutions. Moscow: Infra-M Publ.; 2019. (In Russ.).
- Savchenko EA, Makarova TP. PR and PR-Technologies: Essence, Objectives, Tasks, Functions. *Obrazovanie. Nauka. Nauchnye kadry*. 2019;3:178-180. (In Russ.).
- Skripchenko NYu. The Use of Information and Telecommunication Networks for Criminal Purposes: Regulatory Accounting and Prospects for Expanding Criminal Law Authority. *RUDN Journal of Law*. 2024;28(1):196-214. (In Russ.).
- Vlasova SV. On the question of adapting the criminal procedure mechanism to digital reality. *Biblioteka kriminalista. Nauchny zhurnal*. 2018;1:9-18. (In Russ.).

---

#### ИНФОРМАЦИЯ ОБ АВТОРАХ

**Галяшина Елена Игоревна**, доктор юридических наук, доктор филологических наук, профессор, почетный работник сферы образования Российской Федерации, заведующий кафедрой криминалистики Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)  
д. 9, Садовая-Кудринская ул., г. Москва 125993, Российская Федерация  
eigalyashina@gmail.com

**Комиссарова Ярослава Владимировна**, кандидат юридических наук, доцент, почетный работник сферы образования Российской Федерации, доцент кафедры криминалистики Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)  
д. 9, Садовая-Кудринская ул., г. Москва 125993, Российская Федерация  
a5143836@yandex.ru

---

#### INFORMATION ABOUT THE AUTHORS

**Elena I. Galyashina**, Dr. Sci. (Law), Dr. Sci. (Philology), Professor, Honorary Education Worker of the Russian Federation, Head of the Department of Criminalistics, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation  
eigalyashina@gmail.com

**Yaroslava V. Komissarova**, Cand. Sci. (Law), Associate Professor, Honorary Education Worker of the Russian Federation, Associate Professor, Department of Criminalistics, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation  
a5143836@yandex.ru

Материал поступил в редакцию 23 марта 2024 г.  
Статья получена после рецензирования 11 апреля 2025 г.  
Принята к печати 17 января 2026 г.

Received 23.03.2024.  
Revised 11.04.2025.  
Accepted 17.01.2026.