

ВЫПУСК

№8

НАУЧНЫЙ ПЕРИОДИЧЕСКИЙ  
ЭЛЕКТРОННЫЙ ЖУРНАЛ

# ПРАВОВОЙ АЛЬМАНАХ

2025, октябрь  
№8 (48)

## СПЕЦИАЛЬНЫЙ ВЫПУСК

*«ТЕХНИКО-КРИМИНАЛИСТИЧЕСКИЕ РЕШЕНИЯ ПРОТИВОДЕЙСТВИЯ  
ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ  
ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ»*

*SCIENTIFIC ELECTRONIC PERIODICAL*

**LEGISLATIVE ALMANAC**

2025, October, No. 8 (48)

# ПРАВОВОЙ АЛЬМАНАХ

Октябрь,  
№ 8 (48)  
2025

Научный периодический электронный журнал

Зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (РОСКОМНАДЗОР).  
Регистрационный номер Эл № ФС77-78336

ID журнала: 75537

## Главный редактор:

*МИЛОВАНОВА Марина Михайловна* — доцент кафедры криминалистики Университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук, доцент, г. Москва, Россия

## Ответственный редактор выпуска:

*ВАСИЛЬЕВА Оксана Николаевна* — доцент Департамента правового регулирования экономической деятельности Финансового университета при Правительстве Российской Федерации, кандидат юридических наук, доцент, г. Москва, Россия

## Редакционный совет

*АЛЬБОВ Алексей Павлович* — профессор кафедры теории и истории государства и права Российской таможенной академии, член-корреспондент Российской Академии Естествознания, доктор юридических наук, профессор, г. Москва, Россия

*ВАСИЛЬЕВА Оксана Николаевна* — доцент Департамента правового регулирования экономической деятельности Финансового университета при Правительстве Российской Федерации, кандидат юридических наук, доцент, г. Москва, Россия

*ВИЦЕН Властимил* — проректор Высшей школы экономики и менеджмента публичной сферы в г. Братиславе, доктор философии, доктор права, доцент, г. Братислава, Словацкая Республика

*ГАЙНИШОВА Эдита* — преподаватель юридического факультета Университета имени Я.А. Коменского в Братиславе, доктор философии, доктор права, доцент, г. Братислава, Словацкая Республика

*ЕГОРОВ Николай Николаевич* — профессор кафедры криминалистики юридического факультета Московского государственного университета имени М.В. Ломоносова, доктор юридических наук, профессор, г. Москва, Россия

*КУМАР Абхишек* — PhD, Аллахабадский университет, г. Аллахабад, Уттар-Прадеш, Индия

*ЛЯДОВ Эдуард Владимирович* — профессор кафедры уголовно-исполнительного права Академии права и управления Федеральной службы исполнения наказаний, кандидат юридических наук, доцент, г. Рязань, Россия

*МАНТАРОВА Анна Ивановна* — заведующая кафедрой «Социальный контроль, отклонения и конфликты» Института философии и социологии Болгарской Академии наук, профессор, доктор социологических наук, г. София, Республика Болгария

*НАРУТТО Светлана Васильевна* — профессор кафедры конституционного и муниципального права Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

## Редакционная коллегия

*ЩЕРБАК Евгений Николаевич* — профессор кафедры финансового права Юридического факультета Российского государственного гуманитарного университета, доктор юридических наук, профессор, г. Москва, Россия

*МОЛЧАНОВ Александр Александрович* — профессор кафедры гражданского права и процесса Санкт-Петербургского университета МВД России, доктор юридических наук, профессор, г. Санкт-Петербург, Россия

# LEGISLATIVE ALMANAC

October,  
№ 8 (48)  
2025

*Scientific electronic periodical*

Officially registered at Russian Federal Service of supervision in Communications, IT and Mass Media  
Registration number EI No. FS77-78336 Magazine ID: 75537

## Editor - in-Chief:

*Marina Mikhailovna MILOVANOVA* — Candidate of Law Science, Associate Professor of the Department of criminalistics at Kutafin Moscow State Law University (MSAL), Moscow, Russia

## Executive Editor:

*VASILYEVA Oxana Nikolaevna* — Candidate of Law Science, Associate Professor of Department of Legal Regulation of Economic Activity at Financial University under the Government of the Russia, Moscow, Russia

## Editorial Board

*Alexey Pavlovich ALBOV* — Doctor of Laws, Professor of Department of Theory of State and Law at Moscow Region University, Corresponding Member of Russian Academy of Natural History, Moscow, Russia

*Oxana Nikolaevna VASILYEVA* — Candidate of Law Science, Associate Professor of Department of Legal Regulation of Economic Activity at Financial University under the Government of the Russia, Moscow, Russia

*Vlastimil VICEN* — Doctor of Philosophy, Doctor of Laws, Associate Professor, Vice-Rector at Bratislava High School of Public Affairs Economics and Management, Bratislava, Slovakia

*Edita GAINISHOVA* — Doctor of Philosophy, Doctor of Laws, Associate Professor, Lecturer of Faculty of Laws at Comenius University in Bratislava, Bratislava, Slovakia

*Nikolay Nikolaevich EGOROV* — Doctor of Laws, Professor of the Department of criminalistics of the Faculty of Law at Lomonosov Moscow State University, Moscow, Russia

*Abhishek KUMAR* — PhD, Assistant professor Department of law, University of Allahabad India, Allahabad, Uttar Pradesh, India

*Eduard Vladimirovich LYADOV* — Candidate of Law Science, Associate Professor, Professor of Department of Penal Enforcement Law at Academy under Russian Federal Penal Enforcement Service, Ryazan, Russia

*Anna Ivanovna MANTAROVA* — Head of the Department "Social Control, Deviations and Conflicts" of the Institute of Philosophy and Sociology of the Bulgarian Academy of Sciences, Professor, Doctor of Sociology, Sofia, Republic of Bulgaria

*Svetlana Vasilyevna NARUTTO* — Doctor of Laws, Professor of Department of Constitutional and Municipal Law at Kutafin Moscow State Law University (MSAL), Moscow, Russia

## Editorial Team

*SCHERBAK Evgeniy Nikolaevich* — Doctor of Laws, Professor of the Department of Financial Law of the Faculty of Law of the Russian State University for the Humanities, Doctor of Law, Professor, Moscow, Russia

*MOLCHANOV Alexander Alexandrovich* — Professor of the Department of Civil Law and Procedure, St. Petersburg University of the Ministry of Internal Affairs of Russia, Doctor of Law, Professor, St. Petersburg, Russia

Все статьи рецензируются и публикуются в авторской редакции. За содержание и достоверность статей ответственность несут авторы. Мнение редакции может не совпадать с мнением авторов статей.

При использовании и заимствовании материалов ссылка на издание обязательна. Издание основано в 2020 году.

Материалы журнала включены в систему Научной электронной библиотеки eLibrary.ru

All articles are reviewed and published in original version. All authors are responsible for their content. The editorial board's opinion may not coincide with the author's.

For copying and quoting the link is required.

This magazine was founded at 2020.

All materials are included in Scientific Electronic Library (eLibrary.ru)



Официальный сайт: <https://pravovoyalmanah.ru/jurnal/>  
Official site:  
E-mail: [pravovoialmanah@yandex.ru](mailto:pravovoialmanah@yandex.ru)  
Телефон: +7 (926) 539 67 45  
Phone:

Учредитель и издатель: ООО «Мариокс центр»  
Founder and Publisher: Mariox center llc.

ISSN 2949-060X

ISBN 978-5-6046356-0-5



© ООО «Мариокс центр», 2025  
© Mariox center llc., 2025

**СОДЕРЖАНИЕ**

<b>СЛОВО ГЛАВНОГО РЕДАКТОРА</b> .....	6
<b>Белова К.С.</b> Использование ресурсов сети «Интернет» в решении задач следственного осмотра.....	7
<b>Богатырев К.М.</b> Специфика механизма преступлений, совершаемых посредством коммуникативных действий.....	14
<b>Волохова О.В.</b> Технико-криминалистическое исследование IoT-устройств: цифровые следы и новые возможности.....	21
<b>Галяшина Е.И.</b> Подделка голосовых сообщений в мессенджерах с помощью информационно-коммуникационных технологий: проблемы выявления и исследования (криминалистический аспект).....	28
<b>Кисленко С.Л., Фокин А.Д.</b> Алгоритмы действий следователя в типичных ситуациях первоначального этапа расследования мошенничества в сфере оборота жилых помещений, совершенного с использованием информационно-телекоммуникационных технологий.....	37
<b>Милованова М.М.</b> Технико-криминалистические решения при противодействии преступлениям, совершаемым с использованием информационно-коммуникационных технологий.....	50
<b>Пичугин С.А.</b> Методологические основы использования антропологического подхода в портретной идентификации.....	58
<b>Гололобов Л.С.</b> Некоторые аспекты использования современных информационных технологий в криминалистике.....	66
<b>Карагодина К.Е.</b> Совершенствование технико-криминалистического обеспечения расследования IT-преступлений.....	75
<b>Ушаков Д.А.</b> Проблемы установления обстоятельств противоправных деяний, совершаемых в мессенджерах.....	83



**Марина Михайловна  
МИЛОВАНОВА**

главный редактор  
научного периодического  
электронного журнала  
«Правовой альманах»

## СЛОВО ГЛАВНОГО РЕДАКТОРА

Уважаемые читатели журнала!

Перед вами специальный выпуск научного периодического электронного журнала «Правовой альманах», посвященный технико-криминалистическим решениям при противодействии преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

В представленном тематическом номере журнала опубликованы результаты исследований исполнителей проекта «Фронтирные технико-криминалистические решения для борьбы с современными гибридными угрозами национальной безопасности», а также отдельных участников дизайн-сессии «Технико-криминалистические решения при противодействии преступлениям,

совершаемым с использованием информационно-коммуникационных технологий», проводимой кафедрой криминалистики Университета имени О.Е. Кутафина (МГЮА).

Исследования выполнены в рамках программы стратегического академического лидерства «Приоритет-2030» (Центр компетенций «СОЦИОПРАВО»).

Подготовка и выход в свет специального номера журнала обусловлены необходимостью разработки теоретических положений и основанных на них фронтальных технико-криминалистических решений, обеспечивающих реализацию уголовной политики с целью противодействия и предупреждения преступлений, совершаемых с использованием новых технологий, а также достижения научно-технологического лидерства в соответствующей области.

Тематический номер журнала, опираясь на анализ правоприменительной практики и результаты научных исследований, предлагает разносторонний взгляд на проблему борьбы с преступлениями в сфере информационно-коммуникационных технологий. Авторы публикаций акцентировали внимание на разнообразии средств массовой коммуникации, с одной стороны, и на растущем количестве и многообразии существующих в них рисков, а также специфике совершаемых в информационной среде преступлений, с другой.

Выработанные по результатам проведенных исследований теоретические положения и прикладные рекомендации могут быть использованы в практической деятельности для проведения профилактических мероприятий. Следует подчеркнуть, что в настоящее время как в обществе, так и в профессиональных, экспертных кругах отмечается постепенный переход от технологического оптимизма и энтузиазма в вопросе повсеместного внедрения новых информационно-коммуникативных технологий к более аккуратному, риск-ориентированному подходу в их отношении.

**БЕЛОВА Ксения Сергеевна**

Московский государственный юридический университет имени О.Е. Кутафина (МГЮА),  
преподаватель кафедры криминалистики

[ksbelova@msal.ru](mailto:ksbelova@msal.ru)

125993, Россия, г. Москва, ул. Садовая-Кудринская, 9

**ИСПОЛЬЗОВАНИЕ РЕСУРСОВ СЕТИ «ИНТЕРНЕТ»  
В РЕШЕНИИ ЗАДАЧ СЛЕДСТВЕННОГО ОСМОТРА**

**Аннотация.** В статье рассмотрены отдельные направления использования сети «Интернет» при решении частных задач осмотра. Отмечается, что такие задачи могут быть связаны с использованием как средств навигации для определения точного местоположения устройства, так и интернет-сайтов социальных сетей для поиска фотографий по месту, где они были сделаны. Полученная криминалистически значимая информация будет реализовываться как в виде доказательства, так и ориентирующей информации.

Сформулирован вывод о том, что ресурсы сети «Интернет», применяемые в ходе осмотра, позволяют более детальным образом исследовать обстановку места происшествия и связанные с ним события.

**Ключевые слова:** осмотр, сеть «Интернет», ресурс, общие и частные задачи осмотра, криминалистически значимая информация, сайт, геолокация.

K.S. BELOVA,  
Kutafin Moscow State Law University (MSAL),  
Lecturer of Criminalistics Department  
[ksbelova@msal.ru](mailto:ksbelova@msal.ru)  
9 Sadovaya-Kudrinskaya Str., Moscow, 125993, Russia

**USE OF INTERNET RESOURCES IN RESOLVING INVESTIGATIVE  
INSPECTION PROBLEMS**

**Annotation.** This article discusses certain areas of using the Internet in solving inspection tasks. It is noted that such tasks can be associated with the use of both navigation tools to determine the exact location of the device and online social media sites to search for photos in the place where they were taken. The criminalistically significant information obtained will be implemented both as evidence and orientation information.

**Key words:** inspection, Internet, resource, general and specific inspection tasks, forensically significant information, website, geolocation.

Известно, что одним из самых трудоемких и требующих повышенного внимания со стороны следователя является такое действие, как следственный осмотр. Действующим уголовно-процессуальным законодательством регламентировано, что целью осмотра является обнаружение следов преступления и выяснение других обстоятельств, имеющих значение для уголовного дела. Также в ходе осмотра решаются задачи, связанные с изучением и фиксацией первичной обстановки, в которой было совершено преступление, элементов механизма преступного события и т.д., что в совокупности будет являться как доказательственной, так и ориентирующей информацией по уголовному делу.

Представляется, что изложенные задачи имеют обобщенный характер и не раскрывают специфику частных задач, которые позволяют установить все обстоятельства произошедшего.

В связи с этим Р.С. Белкин справедливо отмечал, что «общей задачей осмотра является выявление всех видов взаимосвязи между местом происшествия и расследуемым преступлением с тем, чтобы по ним в совокупности с другими данными по делу установить механизм происшествия во всех деталях, т.е. ответить на вопрос, что произошло на этом месте. При этом общая задача разбивается на ряд частных, к числу которых относятся:

- непосредственное изучение обстановки для выяснения характера и обстоятельств расследуемого события;
- обнаружение, фиксация, изъятие, предварительное исследование, а также оценка следов преступления;
- получение данных для организации розыска преступника;
- получение исходной информации для выдвижения и проверки версий;
- выявление причин и условий, способствовавших совершению конкретного преступления»<sup>1</sup>.

Общепризнано, что решение общих и частных задач осмотра места происшествия достигается выполнением следователем традиционных действий (применение технико-криминалистических средств и методов для решения задач осмотра, привлечение специалиста и т.п.), по итогам которых составляется протокол осмотра. Однако в силу повсеместного и стремительного развития информационно-телекоммуникационных

---

<sup>1</sup> Белкин, Р.С. Криминалистическая энциклопедия / Р.С. Белкин. — 2-е изд. доп. — М.: Мегатрон XXI, 2000. — 334 с.

технологий, в частности, сети «Интернет», становится целесообразным говорить и об ее применении в решении задач следственного осмотра как частного проявления общей цели<sup>1</sup>, о чем свидетельствуют многочисленные научные публикации<sup>2</sup>.

Проанализировав материалы уголовных дел, а также научные источники, следует сказать о том, что использование сети «Интернет» в решении задач осмотра может быть рассмотрено с двух позиций:

1) осмотр и изъятие электронных носителей информации, которые содержат в себе следы использования ресурсов сети «Интернет» (электронная почта, интернет-страница, мессенджер), как решение общей задачи следственного осмотра;

2) использование отдельных ресурсов сети «Интернет» в ходе следственного осмотра для решения частных задач.

Если же осмотр и изъятие электронных носителей информации регламентированы действующим законодательством и производятся в соответствии со ст. 164.1 УПК РФ, то об использовании ресурсов сети «Интернет» в ходе самого осмотра отсутствует правовая регламентация и, как следствие, возникает вопрос, как и для чего использовать отдельные ресурсы в ходе осмотра.

---

<sup>1</sup> *Мамонов, В.С., Степанов, В.В.* Осмотр места происшествия: правовые, научные основы и практика применения: монография. — М.: Юрлитинформ, 2010. — С. 32-33.

<sup>2</sup> См. например: *Быстряков, Е.Н., Усанов, И.В.* Концепция «следового ядра» и ее применение к системам следов, возникающих в результате киберинцидентов // *Эксперт-криминалист.* — 2023. — № 2. — С. 5-7; *Казакова, А.Н., Меркулова, М.В.* О некоторых проблемах следственного осмотра устройств мобильной связи // *Российский следователь.* — 2023. — № 12. — С. 6-9; *Милованова, М.М.* Современные технико-криминалистические средства и возможности их применения при расследовании преступлений / М.М. Милованова, Т.С. Петранцова // *Legal Bulletin.* — 2020. — Т. 5, № 1. — С. 57-62; *Пичугин, С.А.* Криминалистическое исследование признаков внешнего облика человека, зафиксированных на цифровых носителях / С.А. Пичугин // *Правовое обеспечение суверенитета России: проблемы и перспективы: Сборник докладов XXIV Международной научно-практической конференции и XXIV Международной научно-практической конференции Юридического факультета МГУ им. М.В. Ломоносова в рамках XIII Московской юридической недели. В 4-х частях, Москва, 21–24 ноября 2023 года.* — Москва: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. — С. 303-306; *Скобелин, С.Ю.* Тактика осмотра криминалистически значимой компьютерной информации // *Технологии XXI века в юриспруденции: Материалы седьмой международной научно-практической конференции, Екатеринбург, 05 июня 2025 года.* — Екатеринбург: АНО «Центр содействия развитию криминалистики «КримЛиб»», 2025. — С. 188-193 и др.

В связи с этим считаем необходимым обозначить возможные направления использования сети «Интернет» для решения частных задач осмотра:

1. Использование средств навигации для определения точного местоположения устройства. Согласно Федеральному закону от 14 февраля 2009 г. № 22-ФЗ «О навигационной деятельности», под средствами навигации понимаются технические средства, устройства и системы, предназначенные для формирования навигационных сигналов, передачи, приема, обработки, хранения и визуализации навигационной информации<sup>1</sup>.

В практике расследования встречаются ситуации, когда осмотр или проверка показаний на месте проводятся в местах, отдаленных от каких-либо ориентиров, привязанных к местности. Соответственно, первоначально сложно определить точные данные местоположения участников следственного действия на территории. Такие сведения необходимо устанавливать, поскольку определение места совершения преступления входит в перечень обстоятельств, подлежащих доказыванию. Полагаем, что в решении задачи, связанной с точным определением адресных координат осматриваемой территории, в данном случае можно использовать смартфон с доступом в сеть «Интернет»:

1) посредством использования функции «GPS», позволяющей определять местоположение по координатам сети либо по спутникам GPS. Стоит отметить, что в случае неполадок с сетью определить координаты при отсутствии сигналов от спутников GPS не представляется возможным. Альтернативным, по нашему мнению, будет являться предложение А.В. Рудневского по определению местоположения по базовым станциям GSM-сети<sup>2</sup>;

2) посредством использования специального программного обеспечения/интернет-приложений по определению местоположения устройства (GoogleMaps, TripAdvisor, Моя GPS-позиция и др.). Примечательно, что данные о местоположении мобильного телефона и его перемещении автоматически передаются на серверы компании, которая предоставляет услуги геолокации или сохраняются в памяти

---

<sup>1</sup> Федеральный закон от 14 февраля 2009 г. № 22-ФЗ «О навигационной деятельности» (ред. от 22.07.2024) // Собрание законодательства РФ. — 16.02.2009. — N 7. — ст. 790.

<sup>2</sup> См., например: Рудневский, А.В. Определение местоположения по базовым станциям в сетях GSM // Беспроводные технологии. — 2010. — № 20. — Т.3. — С. 16-18.

телефона. Соответственно, возможности получения сведений о местоположении помогают следователю не только установить точные координаты места, на котором производится следственное действие, но и являются поводом для проведения осмотра смартфона предполагаемого подозреваемого (обвиняемого) и направления его на судебную компьютерную экспертизу с целью обнаружения сведений о местоположении телефона лица в интересующий момент времени с данными, указанными следователем в протоколе осмотра, для установления причастности лица к совершенному преступлению и получения иных доказательств.

Кроме того, указанные интернет-приложения позволяют решать дополнительную задачу по установлению криминалистически значимой информации, когда в рамках подготовки и проведения следственного действия следователь по карте может выявить камеры видеорегистрации, находящиеся вблизи интересующего следствии места, и в последующем получить с них запись того дня, когда происходило расследуемое событие. Например, гр-н А., подозреваемый в убийстве, отрицая свою причастность, в ходе проверки его показаний рассказывал об их с жертвой маршруте движения. Полученные в ходе проверки показаний GPS-координаты не вполне совпадали с координатами отсечек местоположения телефона жертвы в день исчезновения. В последующем обвиняемый А. пояснил, что до момента его задержания он проехал по маршруту дня убийства и специально фиксировал, где находятся камеры уличного наблюдения, под которые он попадал вместе с жертвой, чтобы для возможной проверки показаний выстроить параллельный, не отслеживаемый по камерам маршрут. Если бы органы следствия воспользовались приложением Яндекс-карты, то они обязательно бы обратили внимание, что маршрут проверки его показаний построен так, чтобы объезжать камеры дорожной фиксации, АЗС, торговые комплексы и учреждения<sup>1</sup>.

2. Использование интернет-сайтов социальных сетей для поиска фотографий по месту, где они были сделаны. Довольно часто случайные прохожие или лица, наблюдающие за преступным событием, запечатлевают его на различные устройства, чаще всего фотографируют на мобильные телефоны, после чего публикуют сделанные фотографии на различных ресурсах сети «Интернет», что дает возможность

---

<sup>1</sup> См: уголовное дело № 1-22-13. Архив Тюменского районного суда Тюменской области за 2013 г.

сотрудникам правоохранительных органов искать такие фотографии с целью получения ориентирующей и доказательственной информации по уголовному делу (поиск возможных свидетелей, мест появления подозреваемого (обвиняемого), вероятный маршрут движения и т.д.). Например, необходимо найти фотографии, которые были сделаны неподалеку от места убийства, по адресу: г. Москва, ул. Недорубова, д. 32. Для этого необходимо перейти на сайт <https://vk.com>, открыть свой профиль и выполнить следующие команды: Лента→Поиск→Параметры поиска→Геолокация→Выбираем нужное место на открывшейся карте→Нажимаем на «Искать по записям неподалеку». В поисковом поле появляются необходимые координаты. Копируем их, вставляем в поле для поиска по фото и получаем его. Дальнейшие действия следователя направлены на изучение таких фото и решение вопроса об их использовании в расследовании<sup>1</sup>.

Таким образом, нами предложены направления использования сети «Интернет» для решения частных задач осмотра, что позволяет более детальным образом исследовать обстановку места происшествия и связанные с ним события. Более того, стремительное развитие интернет-технологий открывает возможности развития предложенных и выделения иных направлений их использования для решения задач следственного осмотра, а потому создает перспективы для дальнейших исследований обозначенных в статье вопросов.

#### БИБЛИОГРАФИЯ:

1. *Белкин, Р.С.* Криминалистическая энциклопедия. — 2-е изд. доп. — М.: Мегатрон XXI, 2000. — 334 с.
2. *Быстряков, Е.Н., Усанов, И.В.* Концепция «следового ядра» и ее применение к системам следов, возникающих в результате киберинцидентов // Эксперт-криминалист. — 2023. — № 2. — С. 5-7.
3. *Казакова, А.Н., Меркулова, М.В.* О некоторых проблемах следственного осмотра устройств мобильной связи // Российский следователь. — 2023. — № 12. — С. 6-9.
4. *Мамонов, В.С., Степанов, В.В.* Осмотр места происшествия: правовые, научные основы и практика применения: монография. — М.: Юрлитинформ, 2010. — 184 с.
5. *Милованова, М.М.* Современные технико-криминалистические средства и возможности их применения при расследовании преступлений

---

<sup>1</sup> Аналогичным образом, возможно, производить поиск по геометкам и на иных сайтах социальных сетей или в других ресурсах.

/ М. М. Милованова, Т. С. Петранцова // Legal Bulletin. — 2020. — Т. 5. — № 1. — С. 57-62.

6. Пичугин, С.А. Криминалистическое исследование признаков внешнего облика человека, зафиксированных на цифровых носителях / С.А. Пичугин // Правовое обеспечение суверенитета России: проблемы и перспективы: Сборник докладов XXIV Международной научно-практической конференции и XXIV Международной научно-практической конференции Юридического факультета МГУ им. М.В. Ломоносова в рамках XIII Московской юридической недели. В 4-х частях, Москва, 21–24 ноября 2023 года. — Москва: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. — С. 303-306.

7. Рудневский, А.В. Определение местоположения по базовым станциям в сетях GSM // Беспроводные технологии. — 2010. — № 20. — Т.3. — С. 16-18.

8. Скобелин, С.Ю. Тактика осмотра криминалистически значимой компьютерной информации // Технологии XXI века в юриспруденции: Материалы седьмой международной научно-практической конференции, Екатеринбург, 05 июня 2025 года. — Екатеринбург: АНО «Центр содействия развитию криминалистики «КримЛиб»», 2025. — С. 188-193.

**БОГАТЫРЕВ Константин Михайлович**

кандидат юридических наук

Московский государственный юридический университет имени О.Е. Кутафина (МГЮА),  
старший преподаватель кафедры криминалистики

[kmbogatyrev@msal.ru](mailto:kmbogatyrev@msal.ru)

125993, Россия, г. Москва, ул. Садовая-Кудринская, 9

**СПЕЦИФИКА МЕХАНИЗМА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ  
ПОСРЕДСТВОМ КОММУНИКАТИВНЫХ ДЕЙСТВИЙ**

**Аннотация.** Статья посвящена рассмотрению категории «механизм преступления» применительно к такой категории преступных деяний, как коммуникативные действия, в русле их соотношения с преступлениями, совершаемыми иным образом (в первую очередь — общеуголовными).

В связи с этим рассмотрены и проанализированы подходы к понятию «общеуголовные преступления». Сформулирован вывод о том, что преступления, совершаемые посредством коммуникативных действий, в меньшей степени могут быть отнесены к собственно общеуголовным преступлениям ввиду различия в субъективно оцениваемой степени соответствия формы признанного преступным поведения признаку общественной опасности, а также субъективной оценке совершившим лицом, способе и обстановке совершения деяния, характере следов.

**Ключевые слова:** криминалистика, коммуникация, механизм преступления, общеуголовные преступления, коммуникативные действия.

K.M. BOGATYREV,  
Candidate of Law,  
Kutafin Moscow State Law University (MSAL),  
Senior lecturer of Criminalistics Department  
[kmbogatyrev@msal.ru](mailto:kmbogatyrev@msal.ru)  
9 Sadovaya-Kudrinskaya Str., Moscow, 125993, Russia

**COMMUNICATIVE ACTIONS AS A SPECIAL MECHANISM OF THE  
COMMITTING CRIMES**

**Annotation.** The article deals with the concept of the «mechanism of crime» in perspective of criminal communicative actions. This type of crime is examined in relation to other types of crime such as ordinary crimes.

The concept of «ordinary crimes» is considered and analyzed. The author concludes that communicative actions is a special mechanism of the committing crimes. These crimes differ from ordinary crimes due to the subjectively assessed degree of

*public danger, as well as the subjective assessment of the offender, the manner and setting of the act, and the nature of the traces.*

**Key words:** *criminalistics, communication, crime mechanism, ordinary crimes, communicative actions.*

Существующее многообразие преступных деяний обуславливает необходимость индивидуального подхода к их раскрытию, и расследованию исходя из особенностей, присущих реальным условиям и обстоятельствам их совершения, типичным следам, остающимся на месте происшествия. Специфику реальных преступлений удобно анализировать через призму их механизма — многоплановой динамической системы, включающей самого преступника, его мотив, отношение к своим действиям и к их последствиям; предмет преступного посягательства; способ подготовки, совершения и сокрытия преступления, его обстановку, а также противодействие расследованию со стороны заинтересованных лиц и другие компоненты<sup>1</sup>.

И составы преступлений, предусмотренные Уголовным кодексом РФ, и квалифицируемые в соответствии с его положением конкретные общественно-опасные деяния (преступления) характеризуются чрезвычайным разнообразием, особенно ярко проявляющимся при осуществлении классификации: уголовно-правовой (в первую очередь — по объекту посягательства) либо криминалистической (по любому криминалистически значимому признаку, при выборе которого в качестве основания результирующие группы совместно анализируемых преступлений можно будет изучать эффективно и результативно).

В этом контексте представляет интерес анализ различий механизмов общеуголовных преступлений, являющихся традиционным объектом интереса криминалистов в части разработки методических аспектов их расследования, и иных разновидностей преступлений, отличающихся от упомянутой ранее группы ввиду своей новизны или существенной трансформации со временем.

Следует оговориться, что под общеуголовными преступлениями мы в настоящей работе понимаем общественно опасные деяния лиц, непосредственно посягающих на жизнь и здоровье, неприкосновенность личности, а также на собственность (убийства, изнасилования, кражи, мошенничества, сбыт оружия или наркотиков и т.д.); такие преступления

---

<sup>1</sup> См.: Криминалистика: учебник / под ред. Е.И. Галяшиной, Е.П. Ищенко; отв. ред. Я.В. Комиссарова. — Москва: Проспект, 2025. — С. 14.

характеризуются скорее не спецификой, а массовостью и постоянством в структуре преступности.

Нормативного закрепления данный термин не имеет, однако в научной литературе выработаны и представлены различные подходы к определению данной категории. Так, М.П. Клеймёнов, М.А. Розеенкевич и В.С. Юрьев полагают, что «общеуголовный характер преступлений означает, что это преступления, которые не относятся к экономическим, экологическим, коррупционным, транспортным, компьютерным, политическим, должностным, против порядка управления, воинским, против правосудия, против мира и безопасности человечества»<sup>1</sup>, предлагая затем обширный перечень таких преступлений. В свою очередь, А.И. Игнатов считает, что «общеуголовная преступность представляет собой массовое, системное, криминальное (уголовно запрещенное) поведение части членов общества, не отягощенное, с криминологической точки зрения, другими специфическими объективными (сфера общественных отношений, на которую посягает преступление, жертва преступления, уровень организованности преступной деятельности) и / или субъективными (личность преступника, мотивационная или целевая направленность) характеристиками (признаками)»<sup>2</sup>.

Не вдаваясь в дальнейший анализ существующего многообразия подходов, заключим, что общеуголовные преступления преимущественно определяются через отрицание (перечисление разновидностей преступлений, которые ввиду специфики не относятся к данной категории), а предлагаемые в литературе перечни общеуголовных преступлений носят авторский характер и отражают субъективные представления о том, в каких случаях определенные формы признанного преступным поведения соответствуют признаку общественной опасности, а в каких — нет.

Последнее (постоянство признания за некими деяниями общественной опасности в разных обществах и в разные временные периоды в противовес иным, более контекстуальным основаниям криминализации) может рассматриваться как основной критерий отнесения того или иного преступления к общеуголовным. В этой связи

---

<sup>1</sup> См.: Клеймёнов, М.П., Розеенкевич, М.А., Юрьев, В.С. Общеуголовная нераскрытая преступность // Вестник Омского университета. Серия «Право». — 2010. — № 4 (25). — С. 173.

<sup>2</sup> Игнатов, А.Н. Понятие общеуголовной преступности // Вестник Краснодарского университета МВД России. — 2018. — № 1 (39). — С. 9.

представляется возможным сделать вывод о том, что к общеуголовным преступлениям в меньшей степени возможно отнесение преступлений, совершаемых посредством коммуникативных действий (хотя бы по той причине, что в различных юрисдикциях могут по-разному трактоваться свобода слова и определяться границы правомерного коммуникативного поведения).

Конечно, сходу возникают вопросы, например, к какой категории преступлений в рамках такого подхода будет относиться угроза убийством или причинением тяжкого вреда здоровью (ст. 119 УК РФ) — к общеуголовным или нет? Представляется, что в части механизма преступления между убийством и угрозой убийством имеются разительные различия — и в части способа осуществления, и в части механизма следообразования (в первом случае всегда будут материально-фиксированные следы самого преступления — труп, орудие / оружие, использованное для нанесения повреждений, следы борьбы и т.д., либо следы уничтожения следов; во втором же случае вполне могут остаться лишь идеальные следы). Отношение преступника к своим действиям и к их последствиям также закономерно будет различным (в некоторых ситуациях общения в результате коммуникативной неудачи одной стороной высказывание может восприниматься как шутка, другой же — как реальная угроза).

Другой пример — предусмотренные ст. 135 УК РФ развратные действия: само понятие таких действий в контексте официального толкования является максимально широким и включает любые действия, кроме полового сношения, мужеложства и лесбиянства, совершенные в отношении лиц, достигших двенадцатилетнего возраста (если же данного возраста потерпевший не достиг, то в таком случае будет действовать примечание к ст. 131 УК РФ, и эти деяния будут квалифицированы как изнасилование или насильственные действия сексуального характера), но не достигших шестнадцатилетнего возраста, которые были направлены на удовлетворение сексуального влечения виновного, или на вызывание сексуального возбуждения у потерпевшего лица, или на пробуждение у него интереса к сексуальным отношениям<sup>1</sup>. С точки зрения механизма преступления, квалифицируемые по данной статье, могут разительно отличаться (при том, что характер нарушения половой

---

<sup>1</sup> Постановление Пленума Верховного Суда Российской Федерации от 04.12.2014 № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности» // Российская газета. — № 284. — 12.12.2014.

неприкосновенности несовершеннолетних будет общий): когда физический контакт с телом потерпевшего имел место — ситуация одна, когда развратное действие было совершено с использованием ресурсов сети интернет (например — секстинг в переписке или оголение в видеозвонке) — ситуация иная.

Вместе с тем, помимо ситуаций, в которых коммуникативные действия сопровождают общеуголовные (как, в общем, и иные) преступления или являются их разновидностью, массово имеют место случаи, когда отдельное коммуникативное действие само по себе образует состав преступления (что особенно выражено для формальных составов, где отсутствуют такие элементы, как общественно-опасные последствия и причинно-следственная связь), например: публичные действия, выражающие явное неуважение к обществу и совершенные в целях оскорбления религиозных чувств верующих (ч. 1, 2 ст. 148 УК РФ; указана цель, которая может быть реализовано посредством как вербальной, так и невербальной коммуникации); публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205.2 УК РФ); публичное распространение под видом достоверных сообщений заведомо ложной информации, содержащей данные об использовании Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан (ст. 207.3 УК РФ) и т.д.

В большинстве подобных случаев коммуникация носит компьютерно-опосредованный характер; а учитывая, что сами по себе речевые (и иные коммуникативные) действия в массовом сознании зачастую не воспринимаются как действия, а иногда — как то, за что ответственность в силу наличия свободы слова наступать не должна, становится понятна специфика способа и обстановки совершения таких деяний, а также мотива преступника, его отношения к своим действиям и к их последствиям. Как пишет на этот счет Н.С. Рябинская, «возможность осуществления действий при помощи слов — вопрос не только интенций, но и конвенций. Значение произносимого высказывания и характер совершаемого посредством него действия определяется, во-первых, тем, с каким намерением употребляет говорящий это высказывание, и, во-вторых, тем, каковы конвенции употребления языка для осуществления именно этого типа намерений»<sup>1</sup>.

---

<sup>1</sup> *Рябинская, Н.С.* Речь как социальное действие: основные понятия дискурсивного анализа // Социологический журнал. — 2002. — № 4. — С. 80.

К примеру, если лицо намерено кого-либо похвалить, но выбирает для этого неподходящие средства (не учитывая контекст и личность адресата), то оно рискует оказаться в ситуации конфликта из-за коммуникативной неудачи. И напротив, если человек намеревается угрожать кому-то убийством, но ввиду низкой языковой компетентности или в попытке замаскировать свою цель, выбирает для этого многозначные слова, он рискует быть не понятым (например, его сообщение не будет воспринято всерьез), в то время как следствие рискует принять ошибочное решение об отсутствии состава преступления. Иными словами, для формулирования вывода о преступности деяния необходимо не только установить сам факт его совершения, но и тщательно проанализировать его обстоятельства, формирующие контекст коммуникативной ситуации.

Конечно, общеуголовные преступления (механизм которых подразумевает взаимодействие различных материальных объектов в физическом пространстве с образованием большого количества материально-фиксированных следов) совершаются на порядок чаще; они могут быть охарактеризованы как «вечные», и проблематика их раскрытия и расследования всегда будет оставаться актуальной. Преступления, связанные с совершением коммуникативных действий, напротив — зачастую криминализуются и декриминализуются исходя из текущей конъюнктуры, вызывают множество разногласий касательно того, являются ли они общественно опасными.

Цифровая трансформация изменила коммуникацию, во-многом переместив ее из сферы живого общения в цифровую среду, в которой происходит комбинирование в различных пропорциях устной, письменной и визуальной форм передачи информации (что также не могло не повлиять на механизм слеодообразования)<sup>1</sup>. Свидетельствует об этом и статистика: согласно сведениям, опубликованным МВД России, за январь-декабрь 2024 г. порядка 34 % (649,1 тыс.) от общего числа преступлений были совершены с использованием сети «Интернет»; прирост относительно 2023 г. составил +23,2 %<sup>2</sup>. В связи с этим, остается

---

<sup>1</sup> См.: *Галяшина, Е.И., Богатырев, К.М., Антонян, Е.А., Кокурин, А.В.* Медиабезопасность в цифровой среде: роль сведущих лиц: Монография. — М.: Проспект, 2024. — 288 с.

<sup>2</sup> Состояние преступности в России за январь – декабрь 2024 года // Официальный сайт Министерства внутренних дел Российской Федерации. [Электронный ресурс]. — Режим доступа: URL: <https://мвд.рф/reports/item/60248328> (дата обращения 18.09.2025).

заклучить, что исследование специфики механизма преступлений, совершаемых посредством коммуникативных действий, будет нами продолжено в дальнейших исследованиях.

#### БИБЛИОГРАФИЯ:

1. *Галяшина, Е.И., Богатырев, К.М., Антонян, Е.А., Кокурин, А.В.* Медиабезопасность в цифровой среде: роль сведущих лиц: Монография. — М.: Проспект, 2024. — 288 с.
2. *Криминалистика: учебник / под ред. Е.И. Галяшиной, Е.П. Ищенко; отв. ред. Я.В. Комиссарова.* — Москва: Проспект, 2025. — 512 с.
3. *Клейменов, М.П., Розеенкевич, М.А., Юрьев, В.С.* Общеуголовная нераскрытая преступность // Вестник Омского университета. Серия «Право». — 2010. — № 4 (25). — С. 172-181.
4. *Игнатов, А.Н.* Понятие общеуголовной преступности // Вестник Краснодарского университета МВД России. — 2018. — № 1 (39). — С. 6-10.
5. *Рябинская, Н.С.* Речь как социальное действие: основные понятия дискурсивного анализа // Социологический журнал. — 2002. — № 4. — С. 78-91.

**ВОЛОХОВА Ольга Викторовна***кандидат юридических наук, доцент**Московский государственный юридический университет имени О.Е. Кутафина (МГЮА),  
доцент кафедры криминалистики***olga1416@yandex.ru***125993, Россия, г. Москва, ул. Садовая-Кудринская, 9***ТЕХНИКО-КРИМИНАЛИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ IoT-УСТРОЙСТВ: ЦИФРОВЫЕ СЛЕДЫ И НОВЫЕ ВОЗМОЖНОСТИ**

**Аннотация.** Стремительное распространение интернета вещей (IoT) создало новую цифровую среду, где повседневные устройства (умные колонки, фитнес-трекеры, системы «умного дома» и др.) непрерывно фиксируют детальную информацию о жизни их владельцев, формируя объективную и непрерывную доказательственную базу.

В статье исследуются возможности и методы криминалистического использования данных с IoT-устройств, которые могут выступить «немыми свидетелями» преступлений. Рассматриваются специализированные технико-криминалистические средства и технологии, включая отечественные разработки, и обосновывается необходимость адаптации уголовно-процессуального законодательства и подготовки профильных экспертов для эффективной работы с этим новым источником цифровых следов.

**Ключевые слова:** криминалистика, цифровые следы, интернет вещей (IoT), цифровые доказательства, судебная экспертиза, расследование преступлений.

O.V. VOLOKHOVA,  
Candidate of Law, Associate Professor,  
Kutafin Moscow State Law University (MSAL),  
Associate Professor of the Department of Criminalistics,  
olga1416@yandex.ru  
9 Sadovaya-Kudrinskaya Str., Moscow, 125993, Russia

**TECHNICAL AND FORENSIC EXAMINATION OF IoT DEVICES: DIGITAL TRACES AND NEW OPPORTUNITIES**

**Annotation.** The rapid spread of the Internet of Things (IoT) has created a new digital environment where everyday devices (smart speakers, fitness trackers, smart home systems, etc.) continuously record detailed information about the lives of their owners, forming an objective and continuous evidence base. The article explores the possibilities and methods of criminalistic use of data from IoT devices that can act as «mute witnesses» to crimes. The article considers specialized technical and forensic

*and technologies, including domestic developments, and substantiates the need to adapt criminal procedure legislation and train specialized experts to effectively work with this new source of digital traces.*

**Key words:** *criminalistics, digital footprints, Internet of Things (IoT), digital evidence, forensic examination, crime investigation.*

В настоящее время сложно представить жизнь без информационно-компьютерных технологий. Вместе с тем с их использованием совершаются преступления, и как любые преступления, они оставляют следы, включая и специфические цифровые следы<sup>1</sup>. Однако в одном исследовании невозможно рассмотреть все виды указанных технологий, поэтому остановимся только на IoT-устройствах (Интернет вещей), который стали неотъемлемой частью повседневной жизни, предоставляя пользователям удобство и новые возможности. Интернет вещей — это сеть физических устройств, подключенных к интернету, которые обмениваются данными и управляются с целью облегчения повседневной жизни<sup>2</sup>. Это, например, фитнес-трекеры и умные часы, фиксирующие пульс, местонахождение (GPS), умные колонки (Алиса, Маруся), домашние камеры и датчики, запоминающие движение, открывание дверей, естественно, смартфоны и т.д.

Современные умные устройства постоянно собирают и хранят данные о своей деятельности, создавая цифровой след, который может быть использован в расследовании<sup>3</sup>. Однако их широкое распространение сопровождается, с одной стороны, возможностью их использования в противоправных целях, а с другой — они могут стать «свидетелями» совершенного преступления, что говорит о необходимости разработки методов их криминалистического анализа. При этом в условиях постоянного роста числа подключаемых устройств и их значимости для общества важно учитывать их особенности при проведении расследования. Все это подчеркивает необходимость

---

<sup>1</sup> Барченкова, Я.В. Цифровые следы при расследовании мошенничества, совершенного при помощи средств сотовой связи / Я.В. Барченкова // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. — 2020. — № 4. — С. 135.

<sup>2</sup> Йомудова, Д. Кибербезопасность в мире Интернета вещей: вызовы и возможности / Д. Йомудова, К. Агамаммедов, З. Алладжанова // Ceteris Paribus. — 2023. — № 10. — С. 41.

<sup>3</sup> IoT форензика: как расследовать преступления с помощью умных устройств. — [Электронный ресурс]. — URL: <https://forensicanvil.ru/blog/iot-forensics-smart-devices/> (дата обращения 09.10.2025).

создания специализированных подходов к извлечению и интерпретации цифровых следов, оставляемых IoT-устройствами.

Основная проблема заключается в сложности применения традиционных методов криминалистического анализа и применения технико-криминалистических средств к IoT-устройствам. Стандартные подходы зачастую не позволяют получить полные и достоверные данные, хотя анализ цифровых следов является важным компонентом современного расследования преступлений. Поэтому мы попытаемся акцентировать внимание на криминалистическом анализе цифровых следов, оставляемых IoT-устройствами, способах их извлечения и интерпретации.

Цифровые следы, оставляемые IoT-устройствами, имеют ряд уникальных характеристик, отличающих их от следов, генерируемых традиционными цифровыми устройствами. Особенность этих данных заключается в их высоком уровне детализации, что делает их ценным ресурсом для криминалистического анализа. При этом именно такие особенности создают дополнительные трудности для специалистов, требуя разработки новых подходов к извлечению и интерпретации этих следов.

На формирование цифровых следов в IoT-устройствах влияет множество факторов, включая уровень защиты данных и сложность сетевых взаимодействий. При этом необходимо учитывать, что многие IoT устройства не обеспечивают достаточную защиту данных, что создает риск их несанкционированной модификации или удаления. Также они часто взаимодействуют с облачными сервисами и другими устройствами в сети, что приводит к образованию дополнительного объема данных. Это, например, метаданные о передаче информации, логи<sup>1</sup>, сетевой активности и данные о взаимодействиях между устройствами. При этом такая сложность увеличивает вероятность ошибок при интерпретации данных, что требует от специалистов глубокого понимания структуры IoT-систем и использования современных инструментов и технических средств.

---

<sup>1</sup> Логи — это цифровые записи, на которых в хронологическом порядке фиксируется вся информация о действиях программ, пользователей или системных процессов. Это могут быть записи о событиях, ошибках, запросах, ответах, изменениях или сбоях настроек и т.п., которые происходили в системе.

Конечно, в основном это импортные разработки. Например, Cellebrite UFED 4PC/Physical Analyzer, Magnet AXIOM<sup>1</sup>, являющиеся лидерами рынка, поддерживающие извлечение данных (логи, GPS-треки, показания датчиков) с тысяч моделей смартфонов, планшетов и некоторых умных часов; программы для анализа данных фитнес-трекеров: Fitabase (для Fitbit), или встроенные парсеры в Magnet AXIOM<sup>2</sup>, которые умеют интерпретировать данные о активности и сне из приложений; средства анализа и визуализации извлеченных данных — геоданные: Google Earth Pro, Bulk Location Finder для построения и наложения маршрутов движения подозреваемого на карту, визуализация временных линий: Magnet AXIOM Timeline, X-Ways Forensics для сопоставления активности на разных устройствах в единой хронологии.

Однако и российские ученые, и программисты активно работают в этом направлении, и уже созданы отечественные инструменты, которые могут значительно помочь органам следствия при поиске и анализе различных видов цифровых следов.

Например, Elcomsoft<sup>3</sup>. Это разработчик целой линейки продуктов по цифровой криминалистике. В частности, Elcomsoft iOS Forensic Toolkit — для проведения криминалистического анализа устройств, работающих под управлением Apple iOS; Elcomsoft Phone Breaker — для извлечения и расшифровки данных из резервных копий устройств iOS, Windows Phone и BlackBerry и соответствующих облачных сервисов; Elcomsoft Cloud Explorer — доступ к информации из Google Account; Elcomsoft Explorer for WhatsApp — извлечение, просмотр и анализ истории сообщений пользователей WhatsApp.

Оксиджен софтвер. Это разработчик решений в области аналитики, визуализации для правоохранительных органов. Система «Мобильный

---

<sup>1</sup> Ключ на старт: лучшие программные и аппаратные средства для компьютерной криминалистики. — [Электронный ресурс]. — URL: <https://habr.com/ru/companies/F6/articles/454672/?ysclid=mggi8t01g0919227002> (дата обращения 07.10.2025).

<sup>2</sup> Изучайте цифровые доказательства, полученные с мобильных устройств, из облачных хранилищ, с компьютеров и транспортных средств, а также из сторонних источников, в рамках одного дела. Используйте мощные и интуитивно понятные аналитические инструменты для быстрого автоматического поиска доказательств, имеющих отношение к делу. — [Электронный ресурс]. — URL: <https://www.magnetforensics.com/products/magnet-axiom/> (дата обращения 07.10.2025).

<sup>3</sup> Криминалистический анализ и сбор доказательственной базы. — [Электронный ресурс]. — URL: <https://www.elcomsoft.ru/> (дата обращения 07.10.2025).

Криминалист Эксперт Плюс»<sup>1</sup> позволяет осуществлять криминалистическую экспертизу мобильных устройств, облачных сервисов, компьютеров и дронов.

Интересен и разработчик Belkasoft, у которого есть комплексное решение для цифровой криминалистики Belkasoft Evidence Center X, позволяющее извлекать данные из компьютеров, устройств хранения, дисков и виртуальных машин, памяти, мобильных устройств, облачных сервисов Google, Apple, сервисов мобильной почты, WhatsApp<sup>2</sup>.

Ключевое преимущество российских средств — их фокус на локализованные сервисы. Они могут быть более эффективны для извлечения и анализа данных из таких российских систем, как: Госуслуги, СберБанк Онлайн и приложения других крупных банков, Яндекс.Такси/Еда/Карты, VK, Telegram (хотя последний является международным). Отечественные программы могут иметь более глубокие анализаторы для данных именно этих приложений.

Одним из известных примеров IoT устройств является система Умного дома, которая обладает своей спецификой, в связи с чем и осмотр места происшествия будет отличаться от традиционного способа его проведения. Умный дом фиксирует повседневные действия проживающих в нем людей, их передвижения внутри и другие события, которые сложно зафиксировать другими средствами<sup>3</sup>.

Начинать осмотр места происшествия необходимо начинать с изучения самой системы умного дома, т.е. с набора устройств, которые к ней подключены, включая их настройки. При этом следователь должен убедиться в исправности этих устройств, их активности, подключении к сети. Также обращается внимание на способы доступа к системе: физический или удаленный, например, с помощью мобильного телефона.

К такому осмотру целесообразно привлекать проживающих в нем лиц, если это возможно, специалистов-криминалистов, специалистов по цифровой информации с соответствующим оборудованием, экспертов,

---

<sup>1</sup> Мобильный Криминалист Эксперт Плюс|Каталог Российского ПО. — [Электронный ресурс]. — URL: <https://каталогпо.рф/product/11593> (дата обращения 07.10.2025).

<sup>2</sup> Исследование мобильных устройств в условиях санкций — что принципиально изменилось? — [Электронный ресурс]. — URL: <https://habr.com/ru/articles/736114/?ysclid=mggj74nk4v264644640> (дата обращения 07.10.2025).

<sup>3</sup> Смушкин, А.Б. Отдельные аспекты использования концепции интернета вещей в целях противодействия преступности // Всероссийский криминологический журнал. — 2020. — Т. 14. — № 3. — С. 457- 458.

имеющих квалификацию производства компьютерных экспертиз с необходимыми технико-криминалистическими средствами.

В некоторых случаях возможно привлечение к осмотру и монтажников данной системы Умного дома. Но здесь надо иметь в виду, что они могут иметь личную или иную заинтересованность в расследовании, что скажется на их объективности.

В протоколе осмотра места происшествия фиксируются все обнаруженные устройства, входящие в систему Умного дома, их местоположение и исправность. Кроме этого, необходимо указать в протоколе и наличие традиционных следов: отпечатки пальцев рук (на сенсорных экранах, кнопках, в целом на устройствах), механические повреждения устройств. Особое внимание уделяется камерам видеонаблюдения и сенсорным датчикам, поскольку они содержат данные о времени и действиях, которые могли произойти в период совершения преступления<sup>1</sup>.

Подводя итоги проведенного исследования, можно сказать, что при изучении цифровых следов с IoT устройств необходимо применять комплексные методы их анализа, а интерпретировать полученные данные целесообразно с учетом их специфики и разнообразия. Для этого применяются как «классические» технико-криминалистические средства, так и специальные инструменты и программы.

При исследовании цифровых данных решающее значение имеет привлечение специалистов. Такой подход позволяет следователю, не погружаясь в технические нюансы, понять суть технологий и оставляемых следов и, что важно, их практическую и процессуальную ценность для формирования доказательственной базы.

Дальнейшие исследования в области технико-криминалистического анализа IoT-устройств могут быть направлены на разработку более эффективных инструментов и технологий для обработки данных. Также важно изучение правовых и этических аспектов использования цифровых доказательств, что позволит обеспечить их допустимость в судебных разбирательствах.

---

<sup>1</sup> Хомяков, Э.Г. Устройства умного дома и их значение при расследовании преступлений // Вестник Удмуртского университета. Серия «Экономика и право». — 2025. — №1. — URL: <https://cyberleninka.ru/article/n/ustroystva-umnogo-doma-i-ih-znachenie-pri-rassledovanii-prestupleniy> (дата обращения: 09.10.2025).

**БИБЛИОГРАФИЯ:**

1. *Барченкова, Я.В.* Цифровые следы при расследовании мошенничества, совершенного при помощи средств сотовой связи // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. — 2020. — № 4. — С. 135-138.
2. *Йомудова, Д.* Кибербезопасность в мире Интернета вещей: вызовы и возможности / Д. Йомудова, К. Агамаммедов, З. Алладжанова // Ceteris Paribus. — 2023. — № 10. — С. 63-65.
3. *Смушкин, А.Б.* Отдельные аспекты использования концепции интернета вещей в целях противодействия преступности // Всероссийский криминологический журнал. — 2020. — Т. 14. — № 3. — С. 457- 458.
4. *Хомяков, Э.Г.* Устройства умного дома и их значение при расследовании преступлений // Вестник Удмуртского университета. Серия «Экономика и право». — 2025. — №1. — URL: <https://cyberleninka.ru/article/n/ustroystva-umnogo-doma-i-ih-znachenie-pri-rassledovanii-prestupleniy> (дата обращения: 09.10.2025).

**ГАЛЯШИНА Елена Игоревна**

доктор юридических наук, доктор филологических наук, профессор  
академик РАН

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

**EIGALJASHINA@msal.ru**

125993, Россия, г. Москва, ул. Садовая-Кудринская, 9

## ПОДДЕЛКА ГОЛОСОВЫХ СООБЩЕНИЙ В МЕССЕНДЖЕРАХ С ПОМОЩЬЮ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: ПРОБЛЕМЫ ВЫЯВЛЕНИЯ И ИССЛЕДОВАНИЯ (КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ)

**Аннотация.** В статье рассматриваются наиболее типичные способы подделки голосовых сообщений с помощью технологий синтеза голоса, передаваемых с использованием службы передачи мгновенных сообщений (мессенджеров). Для выявления признаков подмены голоса предлагается использовать разработанные в криминалистике приемы и методы выявления и исследования объектов семиотической природы, запечатленных на цифровых носителях информации.

**Ключевые слова:** криминалистика, клонирование голоса, голосовой синтез, подделка голосового сообщения.

E.I. GALYASHINA,  
Doctor of Law, Doctor of Philology, Professor  
Academician of the Russian Academy of Natural Sciences,  
Kutafin Moscow State Law University (MGUA),  
Head of the Department of Criminalistics  
EIGALJASHINA@msal.ru  
9 Sadovaya-Kudrinskaya Str., Moscow, 125993, Russia

### FORGERY OF VOICE MESSAGES IN INSTANT MESSENGERS USING INFORMATION AND COMMUNICATION TECHNOLOGIES: PROBLEMS OF DETECTION AND RESEARCH (CRIMINALISTIC ASPECT)

**Annotation.** The article discusses the most typical ways of voice messages forgery using voice synthesis technologies, transmitted using instant messaging service (messengers). To identify the signs of voice substitution, it is proposed to use the developed in criminology techniques and methods of identifying and researching objects of semiotic nature, imprinted on digital media.

**Key words:** forensics, voice cloning, voice synthesis, voice message forgery.

Сообщения в мессенджерах сегодня входит в число важных источников криминалистически значимой информации. С ограничением возможностей телефонных звонков по мессенджерам<sup>1</sup> увеличилось число пересылаемых голосовых сообщений (так называемых «войсов»). Этот сдвиг связан с тем, что мессенджеры превратились в ключевой канал коммуникации, позволяя пересылать не только текстовые, но и голосовые сообщения через цифровые платформы.

Однако современные компьютерные технологии позволяют создавать дипфейки — клонировать голос, имея всего несколько фраз. Технологии синтеза речи с использованием ИИ стали доступны для широкого круга пользователей, можно генерировать по образцу длиной в несколько секунд не только монологическую речь конкретных людей, но и целые разговоры с участием нескольких человек без использования монтажа и микширования. При этом обеспечивается относительное разнообразие интонаций, правильная расстановка пауз и фразовых ударений, эмоциональность речи.

Если человек хранит «войсы», то на их основе могут быть сфабрикованы записи якобы от лица конкретного человека. При помощи генеративных технологий можно изготовить подложный текстовый документ, возможна фальсификация вещественного доказательства с целью создания ложного представления о зафиксированном в устной или письменной форме коммуникативном (речевом) событии. В данном случае принято говорить об имитации речевого события при помощи компьютерного моделирования (синтеза голоса и/или речи), поведенческих характеристик реального или вымышленного участника коммуникативного события. Частным случаем такой имитации с использованием технологий искусственного интеллекта выступает так называемый голосовой дипфейк. Имитацию голоса с целью выдать себя за другого человека путем подмены его речевого сигнала с помощью технических средств называют также спуфингом.

Поскольку дипфейки становятся не только проще и дешевле в производстве, но и более реалистичными, все труднее определить, являются ли они поддельными, а вероятность их использования в злонамеренных целях быстро растет. С развитием технологий и повышением их доступности растёт и качество контента, создаваемого

---

<sup>1</sup> Роскомнадзор заявил об ограничении звонков в Telegram и WhatsApp — РБК. — URL: <https://www.rbc.ru/politics/13/08/2025/689c8c7c9a79479b1087586d> (дата обращения 09.09.2025).

генеративными нейронными сетями. Системы искусственного интеллекта, использующие технологии нейронных сетей глубинного обучения, вывели синтез речи на более высокий уровень, имитируя не только стиль и манеру речи человека, но и его когнитивные способности. Это улучшило качество перцептивной узнаваемости говорящего, естественность и разборчивость речи, ее интонационную выразительность, эмоциональность. При этом традиционными методами экспертных исследований (технического исследования) выявить признаки синтезированного голоса не представляется возможным. Более того, существующие экспертные методики не позволяют с достаточной степенью надежности отличить искусственно генерированную устную речь от естественной, особенно это касается монологических голосовых сообщений, пересылаемых в мессенджерах.

Некоторые проблемы выявления подделки голосовых сообщений.

*Анонимность мессенджеров.* Аккаунты зачастую не содержат никаких данных, кроме псевдонима, привязаны к сим-картам, которые могут быть перевыпущены или украдены. Синхронизация переписок между устройствами затрудняет установление лица, отправившего сообщение.

*Редактирование и удаление сообщений.* Многие платформы позволяют редактировать или удалять сообщения даже после их отправки. Скриншоты не отражают эти изменения, если не проведён анализ журналов сервера.

*Шифрование данных.* Мессенджеры с «end-to-end»-шифрованием не хранят данные на серверах, поэтому изъятие информации возможно только с устройства пользователя.

Благодаря современным технологиям достаточно всего 20-секундного фрагмента разговора для создания копии голоса любого человека. Мошенники добывают образцы голоса потенциальной жертвы разнообразными методами: используют общедоступные аудио- и видеозаписи из интернета, а также данные, полученные при утечках биометрической информации. Кроме того, они могут записать голос человека, просто позвонив ему, и использовать диктофон для записи. Иногда мошенники получают доступ к аккаунту пользователя в мессенджере, применяя различные методы, такие как фишинг и социальная инженерия. Получив доступ к переписке, злоумышленники извлекают голосовые сообщения и загружают их в специальную систему, функционирующую на базе ИИ. Эта система затем анализирует голосовые фрагменты и имитирует особенности речи конкретного

человека. В интернете существует множество программ для бесплатного создания аудио-двойников. Можно подделывать голоса знаменитостей или свой собственный, в том числе озвучить заранее подготовленный текст.

Технические особенности мессенджеров несут дополнительные риски для достоверности голосовых сообщений (войсов), предоставляемых по разным категориям дел как доказательство. Так, в частности, в уголовном судопроизводстве при рассмотрении законодательных требований к цифровым доказательствам необходимо учитывать положения ст. 74, 81 и 84 УПК РФ.

По смыслу этих статей голосовые сообщения («войсы») могут быть отнесены к «иным документам» или вещественным доказательствам. Для их проверки в соответствии со ст. 97 УПК РФ требуется сопоставление их с другими доказательствами, имеющимися в уголовном деле, а также установление их источников, получение иных доказательств, подтверждающих или опровергающих проверяемое доказательство. Тогда как для их оценки нужно не только оценить относимость к материалам дела, допустимость (т.е. законность получения), но и достоверность<sup>1</sup>.

Именно последний аспект представляет наибольшую сложность, т.к. отличить синтезированное с помощью ИИ-технологий голосовое сообщение, имитирующее естественную речь конкретного человека, крайне сложно отличить от подлинного (оригинального) продукта речевой деятельности человека («речевого следа»).

Здесь очень важно подчеркнуть, что при изъятии голосовых сообщений принципиально значимым является корректное определение границ исследуемого объекта, то есть вычленение информационного продукта из непрерывного континуума информационного пространства, т.к. коммуникация может носить длянщийся характер, может содержать интертекстуальные включения и гиперссылки, быть частью переписки, где на письменные реплики ответ поступает в виде голосового сообщения и наоборот на голосовое сообщение ответ дается в письменной форме. При этом часть сообщений-реплик может быть пользователями удалена из диалога или полилога в групповом чате. В то же время фрагментарность информации, обусловленная вырезанием части

---

<sup>1</sup> *Галяшина, Е.И.* К вопросу о достоверности криминалистической идентификации личности по цифровым фонограммам устной речи // Известия Тульского государственного университета. Экономические и юридические науки. — 2016. — № 3-2. — С. 19-25.

контента из общего контекста коммуникативной ситуации, чревата ошибками смыслового понимания и неверной интерпретацией при исследовании содержательной стороны сообщения в контексте коммуникативной ситуации.

Текст переписки в мессенджере, в который встроены голосовые сообщения, как максимальная коммуникативная единица несет определенный объем информации, который не является простой суммой его составляющих. Членение речевого коммуникативного акта объясняется психофизиологической организацией человека, который способен одноразово производить и воспринимать периоды, ограниченные по своему объему. Динамика речемыслительного процесса протекает не в равномерно-монотонном ритме, а отдельными связками, квантообразно подобно пульсации звуковой энергии, испускаемой и поглощаемой неравномерными объектами, дискретно, а интонация, будучи неотъемлемой частью любого звучащего текста, одновременно объединяет и разграничивает смысловые отрезки текста. Изучение динамики просодических признаков слитной речи имеет большое значение в распознавании и синтезе речи, верификации и идентификации дикторов, оценке их эмоционального состояния. В процессе коммуникации осуществляется обратная связь, влияющая на поведение человека. Выбор способа общения определяется во многом опытом говорящего, его готовностью к определенному речевому акту, наличием установки, продиктованной отражением объективных условий коммуникации. Коммуникация всегда осуществляется в определенных условиях и обстоятельствах, составляющих ситуацию общения, с учетом тематики речи, степени знакомства говорящего с обсуждаемой проблематикой и т.д.

Ситуативный подход может быть применен для исследования речевых следов преступления в контексте экстралингвистической коммуникативной ситуации, для распознавания продуктов речевой деятельности человека естественного и искусственного происхождения, генерированных с помощью технологий искусственного интеллекта.

Сегодня не все ученые и практики осознают сложность изучения речевой деятельности человека в аспекте ее криминальной имитации, в том числе с использованием современных компьютерных технологий. Зачастую криминалисты упоминают только технические аспекты выявления подделок изображения или голосового подлога, не отдавая должного отражению в речевых следах когнитивных навыков речемыслительной деятельности человека, наиболее сложных для

подражания как другим человеком, так и с помощью искусственного интеллекта<sup>1</sup>. В то же время следы речевой деятельности, запечатленные на материальном носителе, выступают в качестве объектов разнообразных экспертиз (лингвистической, автороведческой, фоноскопической, психологической и др.). Поэтому приоритетными становятся знания в области судебного речеведения, позволяющие не только выявлять в интернет-среде следы «речевых преступлений», но и осуществлять их исследование в целях установления обстоятельств, подлежащих доказыванию по уголовному делу.

Несмотря на то, что системы ИИ, использующие технологии нейронных сетей глубинного обучения, вывели синтез речи на более высокий уровень, воспроизводя голос и отдельные особенности человека, улучшив качество перцептивной узнаваемости говорящего, естественность и разборчивость речи, ее интонационную выразительность, эмоциональность, но они еще не могут имитировать особенности речемыслительной деятельности и когнитивные способности человека. При этом традиционными методами экспертных исследований (технического исследования фонограмм) выявить признаки синтезированного голоса далеко не всегда возможно. Более того, существующие экспертные методики не позволяют с достаточной степенью надежности отличить искусственно генерированную устную речь от естественной, особенно это касается монологических голосовых сообщений, пересылаемых в мессенджерах.

Признаки подделки голосовых сообщений вполне возможно обнаружить при помощи речеведческого исследования (комбинации лингвистических и инструментальных методов визуализации и исследования звучащей речи). Так, например, отличить естественную человеческую речь от синтезированной возможно на основе комплекса просодико-лингвистических признаков, характеризующих речемыслительную деятельность человека. В частности, благодаря методическому подходу по дифференциации спонтанной и

---

<sup>1</sup> *Галяшина, Е.И.* Нейросети — смерть или новая жизнь судебной экспертизы? // Национальные и международные тенденции и перспективы развития судебной экспертизы: Сборник докладов Научно-практической конференции с международным участием, Нижний Новгород, 22–23 мая 2024 года. — Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2024. — С. 83–89.

подготовленной звучащей речи на основе признаков, дифференцирующих различные жанры и стили звучащего текста<sup>1</sup>.

Как указывают эксперты-фоноскописты, синтезированная речь отличается от естественной речи чрезмерной правильностью: чёткая артикуляция, отсутствие признаков ослабления артикуляции, в т.ч. вызванных быстрым темпом произнесения, отсутствие пауз хезитации, а также слов-паразитов, незаконченных слов, сбоев речи, обусловленных обстоятельствами говорения; отсутствие логической и лексико-грамматической перестройки; неоправданных лексических повторов; ошибок словоупотребления; обрывов высказываний, отсутствие или незначительное изменение темпа речи в границах фразы и парентетических внесений, несоответствие лексических конструкций словарному запасу, характерному для диктора, голосом которого воспроизводится текст, совпадения формантной структуры звуков (частотной ориентации формант и динамики их изменения) в одинаковых позициях<sup>2</sup>.

Здесь уместно напомнить, что информация о преступлении как мера связи события и вызванных этим событием изменений в окружающей среде не может существовать без материальной основы, вне информационного сигнала; реализуя преступный замысел, злоумышленник действует в конкретной обстановке, оставляя определенные следы. Следы преступления — любые изменения среды, возникшие в результате совершения в этой среде преступления, т.е. все следы преступления являются материальными. Существуют различные классификации следов в криминалистике. Речевые следы по своей природе можно отнести к знаковым следам. Знаковые системы состоят из однообразно интерпретируемых сигналов, которыми можно обмениваться как по естественным, так и по техническим каналам связи. Знаковые следы для непосредственного восприятия недоступны, т.к. требуют раскодирования в силу того, что знак для получателя информации является условным обозначением какого-либо предмета, объекта или явления<sup>3</sup>.

---

<sup>1</sup> *Галяшина, Е.И.* Судебное речеведение. — М.: НОРМА: ИНФРА-М, 2020. — 320 с.

<sup>2</sup> *Зубов, Г.Н., Зубова, П.И.* Фальсификация звуковой информации с использованием технологий искусственного интеллекта. Особенности технического исследования // Вестник криминалистики. — 2023. — № 3. — С. 5-26.

<sup>3</sup> *Комиссарова, Я.В.* Понятие и классификация следов в криминалистике // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2018. — № 3. — С. 131–141.

К знаковым следам относятся и сведения, передаваемые с помощью машинного кода (языка программирования), с использованием информационно-телекоммуникационных систем, в том числе интернета. Очевидно, что аналоговая или цифровая форма фиксации и хранения криминалистически значимой информации, учитывая скорость научно-технического прогресса (сегодня при передаче информации по оптическим каналам связи используются не только электронные, но и квантовые технологии), в данном случае не имеет значения. В криминалистике на первый план выходит изучение закономерностей порождения криминалистически значимой информации в кодированном виде.

Среди знаковых следов особую группу составляют речевые следы, выраженные в форме устного высказывания, письменного или поликодового сообщения (включающего как вербальный, так и невербальный компоненты), связанные с событием преступления, служащие источником криминалистически значимой информации при раскрытии, расследовании и предупреждении преступлений. Речевые следы фиксируются на материальном носителе, в качестве которого может выступать любой материальный объект (аналоговый, электронно-цифровой), пригодный для запечатления речевых следов в буквенной или звуковой форме. Для криминалистики интерес представляет не только содержательная сторона (содержащаяся в речевом следе информация), но и формальная, отражающая языковую, функционально-стилистическую характеристику сообщения.

Таким образом, криминалистическое исследование подлинности или подделки голосовых сообщений в мессенджерах требует применения специальных речеведческих знаний. Они также востребованы для поиска, обнаружения, фиксации и анализа криминалистически значимой информации о расследуемых речевых преступлениях в информационно-телекоммуникационной среде.

#### **БИБЛИОГРАФИЯ:**

1. *Галяшина, Е.И.* К вопросу о достоверности криминалистической идентификации личности по цифровым фонограммам устной речи // Известия Тульского государственного университета. Экономические и юридические науки. — 2016. — № 3-2. — С. 19-25.
2. *Галяшина, Е.И.* Нейросети — смерть или новая жизнь судебной экспертизы? // Национальные и международные тенденции и перспективы развития судебной экспертизы: Сборник докладов Научно-практической конференции с международным участием, Нижний

Новгород, 22–23 мая 2024 года. — Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2024. — С. 83–89.

3. *Галяшина, Е.И.* Судебное речеведение. — М.: НОРМА: ИНФРА-М, 2020. — 320 с.

4. *Зубов, Г.Н., Зубова, П.И.* Фальсификация звуковой информации с использованием технологий искусственного интеллекта. Особенности технического исследования // Вестник криминалистики. — 2023. — № 3. — С. 5-26.

5. *Комиссарова, Я.В.* Понятие и классификация следов в криминалистике // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2018. — № 3. — С. 131–141.

**КИСЛЕНКО Сергей Леонидович**

доктор юридических наук, доцент

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

профессор кафедры криминалистики

**ser-kislenko@yandex.ru**

125993, Россия, г. Москва, ул. Садовая-Кудринская, 9

**ФОКИН Андрей Денисович**

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

преподаватель кафедры криминалистики

**adfokin@msal.ru**

125993, Россия, г. Москва, ул. Садовая-Кудринская, 9

---

**АЛГОРИТМЫ ДЕЙСТВИЙ СЛЕДОВАТЕЛЯ В ТИПИЧНЫХ  
СИТУАЦИЯХ ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ  
МОШЕННИЧЕСТВА В СФЕРЕ ОБОРОТА ЖИЛЫХ  
ПОМЕЩЕНИЙ, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ  
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ**

**Аннотация.** В условиях цифровизации современной экономики и социума на первый план выходят криминальные способы дистанционного завладения имуществом граждан обманным путем. Это обуславливает сложность в организации расследования мошенничества, совершенного с использованием информационно-телекоммуникационных технологий. Наибольшие трудности следователи испытывают на первоначальном этапе расследования данного вида преступлений.

Проведенный авторами анализ следственной практики позволил типизировать ситуации, складывающиеся на первоначальном этапе расследования данного вида преступлений, и выявить основные проблемы, с которыми приходится сталкиваться следователям.

**Ключевые слова:** мошенничество, недвижимое имущество, методика расследования преступлений, первоначальный этап расследования, криминалистическая ситуация, алгоритм.

S.L. KISLENKO,  
Doctor of Law, Associate Professor  
Kutafin Moscow State Law University (MGUA),  
Professor of the Department of Criminalistics  
ser-kislenko@yandex.ru  
9 Sadovaya-Kudrinskaya Str., Moscow, 125993, Russia

A.D. FOKIN,  
Kutafin Moscow State Law University (MGUA),  
Lecturer at the Department of Criminalistics  
adfokin@msal.ru  
9 Sadovaya-Kudrinskaya str., Moscow, 125993, Russia

**ALGORITHMS OF THE INVESTIGATOR'S ACTIONS IN TYPICAL SITUATIONS OF THE INITIAL STAGE OF THE INVESTIGATION OF FRAUD IN THE SPHERE OF RESIDENTIAL TURNOVER COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES**

**Annotation.** *In the context of the digitalization of the modern economy and society, criminal methods of remote acquisition of citizens' property fraudulently come to the fore. This makes it difficult to organize an investigation of fraud committed using information and telecommunication technologies. Investigators experience the greatest difficulties at the initial stage of investigating this type of crime. The analysis of investigative practice carried out by the authors made it possible to typify the situations that develop at the initial stage of the investigation of this type of crime, and to identify the main problems that investigators have to face.*

**Key words:** *fraud, real estate, crime investigation methodology, initial stage of investigation, criminalistic situation, algorithm.*

В криминалистической литературе традиционно отмечается тесная связь методических рекомендаций с типизацией криминалистических ситуаций, складывающихся в процессе расследования преступлений, от правильной оценки и разрешения которых во многом зависит эффективность деятельности следователя на разных этапах расследования<sup>1</sup>.

---

<sup>1</sup> Белкин, Р.С. Курс криминалистики. Т. 3. — М., 1997. — С. 135; Волчецкая, Т.С. Ситуационный подход в практической и исследовательской криминалистической деятельности: учеб. пособие. — Калининград: БФУ имени И. Канта, 1999. — С. 13; Селиванов, Н.А. Криминалистические характеристики преступлений и следственные ситуации в методике расследования // Социалистическая законность. — 1977. — № 2. — С. 58; Яблоков, Н.П. Следственные ситуации в методике расследования преступлений // Актуальные направления развития криминалистической методики и тактики расследования: матер. расширенного заседания Ученого совета Всесоюзного института по изучению причин и разработке мер предупреждения преступности. — М., 1978. — С. 24.

При этом также очевидна повышенная криминалистическая сложность деятельности следователя в рамках первоначального этапа расследования, характеризующегося необходимостью преодоления проблемного характера следственных ситуаций (обусловленных, как правило, информационной неопределенностью), путем организации следственной работы, направленной на поиск и закрепление источников криминалистически значимой информации о предмете и способе преступления и о лицах, причастных к его совершению.

Выявление и расследование высокотехнологичных преступлений, к которым относится и мошенничество в сфере оборота жилых помещений, совершенного с использованием информационно-телекоммуникационных технологий (далее — ИТТ), как раз и сопряжено с повышенной криминалистической сложностью. Последняя детерминирована: неочевидностью признаков преступной деятельности; нетипичностью следственных ситуаций и сложностями в их интерпретации следователем на первоначальном этапе расследования; трудностями в дифференциации гражданско-правовых и уголовно-наказуемых деяний; отсутствием в большинстве случаев идеальных следов ввиду совершения преступления дистанционным способом, исключающего визуальный контакт преступника и жертвы; трудностями в установлении места окончания преступления, по причине территориальной удаленности преступника и жертвы; проблемностью установления преступников, ввиду использования ими современных возможностей IP-телефонии и других высокотехнологичных средств противодействия их изобличению и пр.

Обобщение следственной практики позволило сформулировать ряд типичных ситуаций, имеющих практическое значение на первоначальном этапе расследования мошенничества в сфере оборота жилых помещений, совершенного с использованием ИТТ<sup>1</sup>:

— потерпевший сообщил о мошенничестве, повлекшем лишение его денежных средств и (или) права на жилое помещение; имеется информация о дистанционном характере оформления сделки с жилым

---

<sup>1</sup> Здесь и далее по тексту приводятся данные, полученные автором по результатам анкетирования сотрудников МВД России, Следственного комитета Российской Федерации, опроса сотрудников агентств недвижимости, нотариусов и помощников нотариусов г. Москвы и Саратовской области, а также анализа следственной и судебной практики по делам о мошенничестве в сфере оборота жилых помещений, совершаемом с использованием информационно-телекоммуникационных технологий в период с 2021 г. по 2025 г.

помещением и переводе денежных средств преступнику, абонентских номерах телефонов (или интернет-ресурсах), использованных для совершения преступления, о банковских счетах, на которые потерпевший перевел денежные средства; данные о свидетелях преступления и информация о личности преступника(ов) отсутствуют;

— потерпевший сообщил о мошенничестве, повлекшем лишение его денежных средств и (или) права на жилое помещение; имеется информация о месте и времени оформления сделки с жилым помещением, передачи денежных средств преступнику, об абонентских номерах телефонов (или интернет-ресурсах), которые были использованы для совершения преступления; имеются сведения о свидетелях преступления и информация о личности преступника(ов);

— потерпевший сообщил о покушении на совершение мошенничества с использованием ИТТ, не повлекшем лишение его денежных средств и (или) права на жилое помещение; имеется информация об абонентских номерах телефонов, с которых поступали звонки потерпевшему; данные о свидетелях преступления и информация о личности преступника(ов) отсутствуют;

— признаки совершения мошенничества с использованием ИТТ были выявлены в ходе оперативно-розыскной деятельности; имеется неполная информация о действиях преступников, повлекших лишение неопределенного круга потерпевших денежных средств и (или) права на жилое помещение; имеется часть информации о потерпевших, свидетелях преступления; имеются признаки деятельности организованной преступной группы.

Для каждой из представленных ситуаций характерен специфический набор и последовательность первоначальных следственных действий и оперативно-разыскных мероприятий. В этом проявляется связь типичных ситуаций расследования с алгоритмами деятельности следователя. Принцип алгоритмизации методики расследования отдельных видов преступлений заключается в практической возможности субъекта расследования в минимальные сроки с помощью несложных операций наметить оптимальные пути переработки исходных данных о следственной ситуации в искомые результаты<sup>1</sup>. При этом процесс программирования деятельности по

---

<sup>1</sup> Шаталов, А.С. Криминалистические алгоритмы и программы. Теория. Проблемы. Прикладные аспекты. — М.: Лига Разум, 2000. — С. 25.

расследованию преступлений детерминируется задачами, стоящими на каждом его этапе.

Первым двум следственным ситуациям, приведенным выше, присущ следующий комплекс первоначальных действий.

Допрос потерпевшего об обстоятельствах произошедшего. Выясняются обстоятельства происшедшего, возможные признаки подозреваемого, а также свидетелей преступного события. При наличии таковых, их следует незамедлительно допросить об обстоятельствах произошедшего. Целесообразно также опросить лиц, проживающих совместно с потерпевшим. От потерпевшего надо получить информацию о том, имеются ли на его компьютерных устройствах программы, препятствующие несанкционированному удаленному доступу, устанавливались ли на данные устройства программы, после которых на них проявлялась подозрительная активность.

Возбуждение перед судом ходатайства о получении сведений о соединениях по абонентскому номеру телефона, с которого, по сведениям потерпевшего, поступали звонки. Вынесение постановления о приобщении полученных документов к материалам уголовного дела. Осмотр распечатки сведений о телефонных соединениях.

Направление запроса в организацию, обслуживающую интернет-ресурс, на котором было размещено объявление о реализации объекта недвижимости (торговые интернет-площадки, социальные сети и пр.) с целью получения сведений о: точном наименовании ресурса; дате и времени размещения объявления; данных, указанных при размещении объявления (номера телефонов, анкетные данные); IP-адреса, с которого осуществлялся вход в учетную запись пользователем, разместившим объявление и пр.; с использованием каких банковских карт (счетов), иных платежных инструментов проводилась оплата за размещение объявления и пр.

Возбуждение перед судом ходатайства о получении сведений о движении денежных средств по абонентскому номеру телефона либо счету банковской карты, используемых субъектом преступления. Приобщение данных документов к материалам уголовного дела и их последующий осмотр. Также, в зависимости от обстоятельств происшедшего, направляются запросы в организации, где предположительно зарегистрированы интернет-кошельки предполагаемых преступников, с целью получения данных клиентов (IP-адреса, с которых происходило открытие кошелька и пр.).

При получении данных об IP-адресах, направляются запросы в адрес провайдеров, которыми были присвоены конкретные IP-адреса в целях получения сведений: о клиентах, которым присвоены IP-адреса; MAC-адресах устройств (логины, пароли, место нахождения устройства, с которого был осуществлен вход в сеть «Интернет») и пр.

Истребование документов по сделке с жилым помещением и сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним: правоустанавливающие документы, документы, подтверждавшие переход права (договора купли-продажи и пр.), сопутствующие документы (справки из БТИ, органов опеки и пр.), доверенности и пр.<sup>1</sup> Данные документы могут быть признаны вещественными доказательствами только после установления связи с событием преступления.

Осмотр мобильного телефона (смартфона) потерпевшего с целью фиксации информации о: IMEI-номере аппарата; абонентских номерах, содержащихся в журнале вызовов мобильного устройства, и СМС-сообщениях в разделе сообщений, внутренней памяти мобильного устройства или SIM-карте; сохраненных текстах переписки между соответствующими абонентскими устройствами (посредством СМС-сообщений или мессенджеров); истории посещения интернет-сайтов и др. Отдельно изучаются разделы приложения «Мобильный банк» (например, «История платежей» и пр.), в которых отражается движение денежных средств по счету. Данная информация при необходимости извлекается, осматривается, описывается и приобщается к протоколу осмотра предмета (телефона) в виде фототаблицы<sup>2</sup>.

Если на момент производства по делу сохранился интернет-ресурс с объявлением о продаже (аренде) жилого помещения, необходимо провести осмотр конкретной интернет-страницы (вместе с потерпевшим) с целью установления и фиксации информации о: точном наименовании сайта; характеристиках размещенного объявления; контактных данных, которые указаны в объявлении; действиях, необходимых для оформления операций с объектом недвижимости, какие данные при этом необходимо ввести на сайте и пр.

---

<sup>1</sup> Слепова, Г. В. Истребование документов при проведении доследственной проверки по факту совершения мошенничества в жилищной сфере // Актуальные проблемы гуманитарных и естественных наук. — 2012. — № 8. — С. 178-183.

<sup>2</sup> Смушкин, А.Б. Цифровизация криминалистической деятельности + eПриложение: дополнительные материалы: учеб. пособие / под ред. В.Б. Вехова. — Москва: КноРус, 2024. — С. 81.

Осмотр места, откуда потерпевший осуществлял выход в сеть «Интернет» (место жительства, общественное место), в котором располагались компьютерные устройства или их системы (компьютер, ноутбук, Wi-Fi роутер, модем и пр.), подключенные к сетям телекоммуникационной связи и содержащие компьютерную информацию.

Осмотр мест расположения банковских терминалов, с помощью которых потерпевший осуществлял перечисление, обналичивание денежных средств. Также необходимо принять меры к своевременному изъятию видеозаписей с камер наблюдения рядом с такими терминалами. Так, в рамках расследования уголовного дела по запросу следователя были изъяты записи с оптического диска с камер видеонаблюдения отделения ПАО «Сбербанк». В ходе их осмотра и последующего допроса подозреваемого С., выполнявшего роль курьера в мошеннической схеме, тот указал на обстоятельства своего нахождения в отделении ПАО «Сбербанк», пояснив что ДД.ММ.ГГГГ. в период времени с 16 час. 45 мин. до 17 час. 02 мин. осуществлял переводы бесконтактным способом неизвестному лицу денежных средств в размере 885 тыс. руб., оставшихся после хищения от денежной суммы в размере 1 млн руб. у пожилого мужчины, который ранее передал данные средства С. на лестничной площадке своей квартиры<sup>1</sup>.

Выемка находящихся у потерпевшего документов, подтверждающих факт перевода денежных средств на другие банковские карты (счета) или лицевые счета, привязанных к абонентским номерам: справки, выписки, чеки, договор на банковское обслуживание карты и пр. Отдельное внимание уделяется документам, присланным преступником (договоры, доверенности, удостоверения личности). Проводится осмотр данных документов.

Поручение органу дознания проведения оперативно-разыскных мероприятий с целью установления лиц, причастных к преступлению (например, проверка абонентских номеров телефонов или счетов банковских карт подозреваемых лиц на совпадение по другим уголовным делам, преступления по которым совершены аналогичным способом; проверка данных лиц и аналогичных преступлений по системе «Дистанционное мошенничество»<sup>2</sup> и пр.). В случае получения

---

<sup>1</sup> Приговор Гагаринского районного суда г. Севастополя № 1-339/2024 от 03.06.2024 по делу № 1-339/2024 // СудАкт. — [Электронный ресурс]. — URL: <https://sudact.ru/regular/doc/EWQQy7BfbB5T/> (дата обращения: 12.10.2025).

<sup>2</sup> Была введена приказом ГУ МВД России по г. Москве от 05.04.2021 № 121.

информации о том, что подозреваемый зарегистрирован за пределами региона, рекомендуется сообщить об этом в Управление уголовного розыска МВД России соответствующего региона с целью последующего направления в установленный регион телеграммы<sup>1</sup>.

При наличии соответствующих объектов назначаются необходимые судебные экспертизы.

Как можно заметить, эффективность первоначальных (особенно доследственных) действий во многом зависит от эффективности взаимодействия и обмена данными между правоохранительными органами и банками<sup>2</sup>, а также иными структурами, которые могут быть задействованы в реализации мошенничества, совершенного с использованием ИТТ. Такое взаимодействие, на наш взгляд, немыслимо без принятия соответствующих мер, направленных на сокращение сроков исполнения запросов правоохранительных органов (в адрес кредитных организаций, операторов сотовой связи и др.). Немаловажное значение имеет повышение оперативного доступа и использования следователями информации, содержащейся в цифровых базах соответствующих организаций.

Правоприменителям необходимо учитывать, что такая информация не хранится длительное время. Так, сроки хранения фото- и видеоизображений в банкоматах устанавливаются внутренним регламентом конкретной кредитной организации и, в среднем, составляют от одного до двух месяцев. В этом плане мы разделяем позицию А.И. Бастрыкина о том, что лицо, производящее расследование должно иметь оперативный доступ к базам данных и интернет-ресурсам Центрального банка России, Федеральной нотариальной палаты и др.<sup>3</sup> Представляется, что это возможно только при активном внедрении в

---

<sup>1</sup> Аксенова, Л.Ю. Алгоритм действий следователя и органа дознания при расследовании мошенничеств с использованием средств сотовой связи // Вестник Омской юридической академии. — 2016. — № 3. — С. 83.

<sup>2</sup> В частности, с 2023 г. сотрудники МВД России могут оперативно получать данные об операциях без согласия клиента из автоматизированной системы ФинЦЕРТ (Центр взаимодействия и реагирования Департамента информационной безопасности) Банка России. Информацию, полученную от правоохранительных органов, банки смогут учитывать для предотвращения новых мошеннических операций (Федеральный закон от 20.10.2022 № 408-ФЗ «О внесении изменений в статью 26 Федерального закона «О банках и банковской деятельности» и статью 27 Федерального закона «О национальной платежной системе» // Собрание законодательства РФ. — 24.10.2022. — № 43. — Ст. 7271).

<sup>3</sup> Бастрыкин, А.И. Цифровые технологии современной криминалистики // Вестник Академии Следственного комитета РФ. — 2021. — № 2. — С. 16.

организацию процесса расследования анализируемых преступлений механизмов частно-государственного партнерства (в том числе в рамках использования технологии OSINT<sup>1</sup>).

В третьей следственной ситуации из числа вышеуказанных, когда имеются признаки покушения на мошенничество с использованием ИТТ, алгоритм первоначального этапа расследования дополняется следующими действиями.

Проведение оперативно-разыскных мероприятий, направленных на получение информации о криминальной деятельности преступника(ов): прослушивание телефонных переговоров, получение компьютерной информации и пр. Отдельное внимание, как рекомендуется в литературе, необходимо уделить получению образцов голоса для сравнительного исследования<sup>2</sup>. Это позволит в последующем использовать их для идентификации преступников в рамках фоноскопической экспертизы.

Проверка и истребование информации о преступнике и месте его жительства по базам ИЦ и ГИАЦ.

Организация тактической операции по задержанию мошенника. Здесь немаловажное значение приобретает инструктаж заявителя о преступлении с целью побудить преступников получить денежные средства наличными, а также оперативное сопровождение возможных посредников (курьеров) при передаче данных денежных средств. Так, по заявлению потерпевшей было установлено, что мошенники, представившись сотрудниками правоохранительных органов, обманным путем пытаются получить от нее 1 млн руб. Оперативниками было установлено, что преступники за деньгами, скорее всего, пришлют стороннего курьера одной из служб доставки. Было решено сделать муляж пакета с деньгами и проследить, кому в итоге отвезут деньги. Преступники заказали такси-доставку. Потерпевшая передала водителю пакет с муляжом денег, а оперативники проследили за машиной. После

---

<sup>1</sup> OSINT (Open Source Intelligence) — комплекс мероприятий, инструментов и методов для получения и анализа информации из открытых источников. (Подробнее см.: Миширяков, И.В., Шевелев, А.Д., Макачук, Д.В., Жданова, М.М. Исследование инструментов и методов для сбора и анализа открытой информации в сети Интернет (OSINT) // Вестник науки. — 2024. — Т. 3. — № 6. — С. 1414–1422).

<sup>2</sup> Щербаченко, А.К. Алгоритмы оперативно-разыскного обеспечения раскрытия дистанционных мошенничеств, совершенных группой лиц // Философия права. — 2022. — № 1. — С. 144-150.

остановки автомобиля, к нему подошел молодой человек, который забрал пакет, был задержан<sup>1</sup>.

Допрос задержанных лиц с целью установления их причастности к преступному деянию и выяснения обстоятельств его совершения. Такие допросы дифференцируются в зависимости от установления роли задержанного в мошеннической схеме. Так, при допросе курьеров рекомендуется выяснить: когда, где, в каком размере он получал денежные средства; как распорядился этими средствами; по чьей просьбе получал денежные средства; как и кто ему объяснил просьбу получить денежные средства, может ли он дать подробное описание внешности данного лица, знал ли, что деньги получены преступным путем и пр.<sup>2</sup> При допросе подозреваемого, относящегося к техническому персоналу, следует выяснить сведения о: времени создания и действия интернет-сайта или размещения объявления о продаже (аренде) недвижимости; программном обеспечении, использованном для создания сайта; способах связи с потенциальными клиентами, используемых абонентских номерах телефонов и пр.

Проведение обысков в жилище подозреваемого лица с целью обнаружения и изъятия: компьютерной техники, устройств телекоммуникации (Wi-Fi роутера, модема), средств мобильной связи; документов, содержащих сведения, которые относятся к этапам подготовки, совершения и сокрытия хищений денежных средств с информационно-телекоммуникационных технологий (в том числе бухгалтерские записи преступников). Отдельное внимание с учетом вида рассматриваемого мошенничества в литературе рекомендуется обращать на обнаружение (в том числе в памяти электронных источников информации) текстов обращений к жертвам, сценарии и алгоритмы обмана, рекомендации по оказанию психологического воздействия и т.п.<sup>3</sup>

---

<sup>1</sup> Московская домохозяйка организовала спецоперацию по задержанию телефонных мошенников: «Я поняла, что должна их поймать» // Комсомольская правда. — [Электронный ресурс]. — URL: <https://www.kp.ru/daily/28322/4465249/> (дата обращения: 12.10.2025).

<sup>2</sup> Аксенова, Л.Ю. Алгоритм действий следователя и органа дознания при расследовании мошенничеств с использованием средств сотовой связи // Вестник Омской юридической академии. — 2016. — № 3. — С. 84.

<sup>3</sup> Старостенко, Н.И. Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий: автореф. дис. ... канд. юрид. наук. — Краснодар, 2023. — С. 26.

В ситуации выявления признаков совершения мошенничества с использованием ИТТ в процессе проведения оперативно-разыскной деятельности, актуализируются следующие направления:

— выяснение круга возможных потерпевших от действий преступников и проверка потерпевших по аналогичным преступлениям по информационным базам;

— проведение мероприятий в целях проверки лиц, состоящих на учетах в органах внутренних дел, а также лиц, в отношении которых получены сведения о возможной причастности к совершению преступления, в целях выяснения, не совершались ли мошенничества аналогичным способом или сходными по приметам лицами на территории других ОВД;

— анализ оснований для принятия решения об объединении дел в одно производство;

— изучение материалов и стенограмм прослушивания телефонных переговоров и иных сообщений преступников, оперативного наблюдения с приобщенными фото- и видеокадрами и пр.;

— установление всех участников преступления и лиц, причастных к его совершению;

— розыск преступников (в том числе посредством задействования различных видов криминалистических учетов) и организация проведения иных ОРМ (наведение справок, сбор образцов для сравнительного исследования, исследование предметов и документов, наблюдение, обследование помещений, зданий, сооружений, участков местности и транспортных средств и др.);

— направление запроса о выдаче лица, находящегося на территории иностранного государства (ст. 460 УПК РФ).

Организация расследования в рамках последующих этапов сопряжена с проведением следственных действий, направленных на усиление доказательственной базы по уголовному делу: допросы подозреваемых (при наличии) и посредников, участвовавших в криминальной схеме, а также свидетелей (представители регистратора доменных имен, провайдера хостинга, сотрудники банков и кредитных организаций); назначение и производство необходимых экспертиз (компьютерно-технической, психологической, комплексной психолого-психиатрической, психолого-лингвистической, судебно-технической экспертизы документов, трасологической и пр.); предъявление для опознания лиц и предметов; направление запросов регистратору

доменного имени с целью аннулирования домена сайта мошеннического интернет-ресурса и т.д.

### БИБЛИОГРАФИЯ:

1. *Аксенова, Л.Ю.* Алгоритм действий следователя и органа дознания при расследовании мошенничеств с использованием средств сотовой связи // Вестник Омской юридической академии. — 2016. — № 3. — С. 80-84.
2. *Бастрыкин, А.И.* Цифровые технологии современной криминалистики // Вестник Академии Следственного комитета РФ. — 2021. — № 2. — С. 15-19.
3. *Белкин, Р.С.* Курс криминалистики: в 3 т. Т. 3: Криминалистические средства, приемы и рекомендации. — Москва: Юристъ, 1997. — 480 с.
4. *Волчецкая, Т.С.* Ситуационный подход в практической и исследовательской криминалистической деятельности: учеб. пособие. — Калининград: БФУ имени И. Канта, 1999. — 74 с.
5. *Мищиряков, И.В., Шевелев, А.Д., Макарчук, Д.В., Жданова, М.М.* Исследование инструментов и методов для сбора и анализа открытой информации в сети Интернет (OSINT) // Вестник науки. — 2024. — Т. 3. — № 6. — С. 1414-1422.
6. *Селиванов, Н.А.* Криминалистические характеристики преступлений и следственные ситуации в методике расследования // Социалистическая законность. — 1977. — № 2. — С. 56-59.
7. *Слепова, Г.В.* Истребование документов при проведении доследственной проверки по факту совершения мошенничества в жилищной сфере // Актуальные проблемы гуманитарных и естественных наук. — 2012. — № 8. — С. 178-183.
8. *Смушкин, А.Б.* Цифровизация криминалистической деятельности + eПриложение: дополнительные материалы: учеб. пособие / под ред. В.Б. Вехова. — Москва: КноРус, 2024. — 198 с.
9. *Старостенко, Н.И.* Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий: автореф. дис. ... канд. юрид. наук. — Краснодар, 2023. — 29 с.
10. *Шаталов, А.С.* Криминалистические алгоритмы и программы. Теория. Проблемы. Прикладные аспекты. — М.: Лига Разум, 2000. — 252 с.
11. *Щербаченко, А.К.* Алгоритмы оперативно-разыскного обеспечения раскрытия дистанционных мошенничеств, совершенных группой лиц // Философия права. — 2022. — № 1. — С. 144-150.
12. *Яблоков, Н.П.* Следственные ситуации в методике расследования преступлений // Актуальные направления развития криминалистической методики и тактики расследования: матер.

расширенного заседания ученого совета Всесоюзного института по изучению причин и разработке мер предупреждения преступности. — М., 1978. — С. 24-30.

**МИЛОВАНОВА Марина Михайловна**

кандидат юридических наук, доцент

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

доцент кафедры криминалистики

Главный редактор научного периодического электронного журнала  
«Правовой альманах»

[mmmilovanova@msal.ru](mailto:mmmilovanova@msal.ru)

125993, Россия, г. Москва, ул. Садовая-Кудринская, 9

## ТЕХНИКО-КРИМИНАЛИСТИЧЕСКИЕ РЕШЕНИЯ ПРИ ПРОТИВОДЕЙСТВИИ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

**Аннотация.** *Общественно опасные деяния, совершаемые с использованием информационно-коммуникационных технологий или в сфере компьютерной информации (киберпреступления), представляют серьезную угрозу национальной безопасности Российской Федерации. В связи с этим вопросы обеспечения кибербезопасности и противодействия мошенничеству сегодня приобрели особую актуальность и вышли за рамки узкопрофессиональной повестки.*

*В статье отмечается, что криминалистическая превенция в этом отношении является приоритетным направлением в решении данных вопросов, а успешная деятельность правоохранительных органов в борьбе с киберпреступлениями немыслима без использования продуманной системы криминалистических средств профилактического характера, отвечающих современным потребностям общества.*

*Предложено авторское понятие киберпреступлений, проанализированы современные возможности и технико-криминалистические решения противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий. В качестве такового решения отмечается целесообразность использования искусственного интеллекта (ИИ) и Антифрод-системы как перспективных инструментов, позволяющих правоохранителям не только раскрывать, но и предупреждать рассматриваемые преступления, осуществлять обработку больших объемов информации, поиск связей субъектов преступной деятельности, выявление подозрительных действий, создание криминальных портретов, карт.*

**Ключевые слова:** *киберпреступления, криминалистическая превенция, криминалистическая профилактика, противодействие информационной безопасности, искусственный интеллект (ИИ), Антифрод-системы.*

M.M. MILOVANOVA,  
Candidate of Law, Associate Professor,  
Kutafin Moscow State Law University (MSAL),  
Associate Professor of the Department of Criminalistics,  
mmmilovanova@msal.ru  
9 Sadovaya-Kudrinskaya Str., Moscow, 125993, Russia

**ON THE ISSUE OF THE CONCEPT OF PROCUREMENT FOR STATE AND MUNICIPAL NEEDS AND THE MAIN TYPES OF CRIMES COMMITTED IN THIS AREA**

**Annotation.** *Socially dangerous acts committed using information and communication technologies or in the field of computer information (cybercrime) pose a serious threat to the national security of the Russian Federation. In this regard, the issues of ensuring cybersecurity and countering fraud have become particularly relevant today and have gone beyond the narrow professional agenda. The article notes that criminalistic prevention in this regard is a priority in addressing these issues, and the successful work of law enforcement agencies in combating cybercrime is unthinkable without the use of a well-thought-out system of forensic preventive measures that meet the modern needs of society. The author's concept of cybercrime is proposed, modern possibilities and technical and criminalistic solutions for countering crimes committed using information and communication technologies are analyzed. As such, it is noted that it is advisable to use artificial intelligence (AI) and an Anti-fraud system as promising tools that allow law enforcement officers not only to uncover, but also to prevent crimes under consideration, process large amounts of information, search for connections between subjects of criminal detail, identify suspicious actions, create criminal portraits, maps.*

**Key words:** *cybercrime, forensic prevention, forensic prevention, countering information security, artificial intelligence (AI), Anti-fraud systems.*

Сегодня сложно представить современное общество без информационных технологий, которые приобрели глобальный, трансграничный характер и стали неотъемлемой частью жизни граждан, общества и государства. Информационные технологии трансформируют устоявшиеся процессы и создают новые возможности в различных сферах экономики, улучшают качество жизни людей, обеспечивают их коммуникацию и досуг.

Вместе с тем формирование информационного общества и активное внедрение информационных технологий не могло обойти стороной криминально настроенных граждан, деятельность которых создает угрозу информационной безопасности. Возможности трансграничного оборота информации всё чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских,

криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности<sup>1</sup>.

Опасность нанесения ущерба национальным интересам в информационной сфере требует разработки взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления, что определено в качестве стратегических целей и основных направлений обеспечения информационной безопасности в Доктрине об информационной безопасности Российской Федерации.

Обеспечение информационной безопасности является одним из важнейших направлений деятельности правоохранительных органов. Вместе с тем, Президент Российской Федерации В.В. Путин в своем выступлении на ежегодном расширенном заседании коллегии Министерства внутренних дел Российской Федерации посвященной итогам работы органов внутренних дел за 2024 год, а также приоритетным задачам на текущий, 2025 год отметил, что количество преступлений, совершённых с использованием информационных технологий растёт, а их раскрываемость снижается. При этом глава государства акцентировал внимание на ущербе от киберпреступлений, который превысил 200 миллиардов рублей с учетом того, что четверть обманутых и пострадавших людей — это пенсионеры<sup>2</sup>.

Действующим уголовным законодательством главой 28 УК РФ предусмотрена уголовная ответственность за совершение преступлений в сфере компьютерной информации: неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 272 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 272 УК РФ). Обозначенные

---

<sup>1</sup> Пункт 7 «Доктрины об информационной безопасности Российской Федерации». См.: Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. — 12.12.2016. — № 50. — ст. 7074.

<sup>2</sup> Расширенное заседание коллегии МВД РФ от 5 марта 2025 года. Сайт Президента РФ. [Электронный ресурс]. Режим доступа URL: <http://www.kremlin.ru/events/president/transcripts/deliberations%20/76408> (дата обращения 20.09.2025 г.).

противоправные деяния напрямую затрагивают сферу информационно-коммуникационных технологий. Вместе с тем законодателем в Уголовный закон включена формально не относящаяся к главе 28 статья 159.6 УК РФ, регламентирующая ответственность за мошенничество в сфере компьютерной информации, а также статья 159.3 УК РФ — мошенничество с использованием электронных средств платежа. Кроме того, следует отметить, что на сегодняшний день достаточно распространенными имущественными преступлениями, совершаемыми с использованием информационных технологий, являются деяния, предусмотренные п. «г» ч. 3 ст. 158 УК РФ — кража, совершённая с банковского счета.

В контексте рассматриваемого вопроса под преступлениями в сфере информационных технологий (киберпреступлениями) предлагается понимать любые противоправные деяния, совершаемые в отношении информации, обрабатываемой и используемой в киберпространстве — среде, которая создана в результате взаимодействия людей, программного обеспечения и услуг в сети Интернет с помощью технологических устройств и подключённых к нему сетей.

Вместе с тем необходимо учитывать, что современные достижения в сфере информационных технологий, новые возможности применения беспроводных технологических решений и искусственного интеллекта, который уже сейчас конкурирует с человеком во многих сферах, а также анализ перспектив развития IT-отрасли позволяет спрогнозировать появление новых видов (как минимум способов) киберпреступлений с использованием цифровой информации. Такой прогноз обусловлен фактами активного использования криминально настроенными субъектами технически сложных устройств, информационных систем, компьютерных сетей, Интернета для достижения преступных целей в процессе реализации противоправной деятельности. В этой связи органы государственной и исполнительной власти и, в частности, правоохранительные органы должны своевременно, оперативно реагировать на эти вызовы, в том числе работая на опережение. При этом приоритетным направлением государственной политики в борьбе с киберпреступлениями должна стать их профилактика, предупреждение на ранних стадиях с целью не допустить наступления тяжких последствий.

Представляется, что профилактика рассматриваемых преступлений — важное направление криминалистики, требующее различных специальных мер, направленных не только на предотвращение и пресечение киберпреступлений, но и на устранение причин и условий, способствующих их совершению. В качестве такого решения для противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий на сегодняшний день, может выступать искусственный интеллект (ИИ) как перспективный инструмент, позволяющий правоохранителям не только раскрывать, но и предупреждать рассматриваемые (и не только) преступления, используя его для обработки больших объёмов информации, поиска связей, выявления подозрительных действий, создания криминальных портретов и карт.

Несмотря на то, что на сегодняшний день отсутствует единообразное понятие ИИ, в качестве его основных признаков можно выделить: во-первых, способность к самообучению, что отличает ИИ от обычных программ (приложений), обуславливая схожесть с человеком; во-вторых, способность принимать решения на основе имеющихся данных; в-третьих, способность к анализу и обработке большого объёма данных. Соответственно, под ИИ можно понимать совокупность аппаратно-программных, программно-технических, технологических средств и методов, накопленной информации, позволяющих пользователю решать определённые задачи. В контексте рассматриваемого вопроса — это задачи, связанные с повышением эффективности деятельности правоохранительных органов по раскрытию, расследованию и предупреждению преступлений и иных правонарушений.

Примером применения ИИ в анализе данных для предупреждения преступлений в нашей стране служит система «Криминалист», позволяющая анализировать информацию из баз данных МВД, ФСБ, ФСИН, СКР, ФНС, Росфинмониторинга и др. и из открытых источников — социальных сетей, СМИ и как следствие обнаруживать потенциальных преступников, места совершения преступлений. Система также способна предлагать оптимальные решения для сотрудников правоохранительных органов.

Представляется, важную роль в деле обеспечения кибербезопасности и создания единого цифрового «щита» страны против мошенников способны сыграть Антифрод-системы, которые находят

применение в сферах, где используются онлайн-сервисы и дистанционное обслуживание, включая кредитные организации, госсектор, телекоммуникации, электронную коммерцию и др. Принцип их работы фокусируется на обнаружении подозрительных действий после того, как все формальные проверки безопасности уже пройдены, что особенно актуально в ситуациях, когда субъекты преступной деятельности используют легитимные учётные данные, действительные платежные реквизиты или заранее созданные аккаунты для обхода стандартных защитных мер.

В этой ситуации единственный метод обнаружения атаки — изучение поведения пользователя: кто совершает действия, какие именно, с какого устройства, откуда, в какое время и насколько это отклоняется от обычного шаблона. В качестве иллюстрации можно привести ситуацию, когда мошенник пытается войти в аккаунт клиента банка, используя мобильное приложение с типичного устройства. При успешной верификации, как правило, моментально начинается проведение транзакций, связанных с переводом денежных средств на счета, которые ранее были замечены в мошеннических действиях, причём геолокация этих счетов не соответствует территориальному нахождению клиента. Такие транзакции на основе совокупности факторов риска за счёт комплексной системы Антифрод блокируются, и уже до завершения операции данные об инциденте передаются на детальное рассмотрение специалистам службы безопасности.

Анализ российского рынка Антифрод-систем позволяет говорить, что уже сегодня алгоритмы машинного обучения способны распознавать сложные финансовые мошеннические схемы, когда транзакции на первый взгляд не кажутся подозрительными, но отклоняются от обычного шаблона использования карты держателем. Такие системы позволяют выявлять использование неизвестного устройства, нестандартного браузера или нетипичное время проведения транзакции. Для верификации при необходимости могут запрашиваться дополнительные сведения для подтверждения личности. При этом, к примеру, профилактическая цель использования транзакционного Антифрода состоит в анализе финансовых операций, выявлении подозрительной активности, превышении определенного лимита, нетипичных для клиента частоты проведения операций и территориальных зонах. В свою очередь, сессионный, или браузерный Антифрод способен анализировать технические аспекты пользовательской сессии, такие как используемое устройство, параметры подключения к интернету, поведенческие реакции

пользователя (например, движение курсора мыши, скорость набора текста).

Обозначенные системы вполне подходят для решения задач выявления компрометации учетных записей и фишинговых атак на ранних стадиях, когда подозрительное поведение мошенника, действовавшего от лица пользователя, проявляется не только в финансовых операциях. Возможности сессионных и транзакционных решений могут сочетать гибридные Антифрод-системы, в которых применяются как заранее заданные установки и фильтры, так и сложные алгоритмы машинного обучения, позволяющего существенно сократить время реагирования на подозрительные транзакции, а используемые автоматизированные системы — мгновенно блокировать подозрительные операции и транзакции, что минимизирует финансовые потери для участников правоотношений<sup>1</sup>. Внедрение технологий машинного обучения в Антифрод-системы должно стать надёжной защитой от растущих киберугроз.

Резюмируя изложенное, можно констатировать, что ИИ, и, в частности, Антифрод-системы целесообразно использовать в качестве средства противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий. Это программные решения, разработанные для выявления и предотвращения мошеннических действий в финансовых операциях, в основе которых лежит анализ множества параметров каждой операции с последующей оценкой её достоверности, включая сумму платежа, уникальный идентификатор пользователя, IP-адрес, историю отклоненных транзакций и др.

Способность алгоритмов машинного обучения выявлять закономерности, указывающие на противоправное поведение, и их возможность предупреждать нарушения могут использоваться правоохранителями как инструмент борьбы с финансовым мошенничеством в масштабах государства. Перспективы внедрения государственной информационной системы (ГИС) «Антифрод» определены на ближайшее будущее (она должна быть создана на базе

---

<sup>1</sup> *Плотников, И.* Обзор рынка систем противодействия мошенничеству (anti-fraud, антифрод). — [Электронный ресурс]. — Режим доступа: URL: [https://www.anti-malware.ru/analytics/Market\\_Analysis/Anti-Fraud?ysclid=mgtsbds8hl137030979](https://www.anti-malware.ru/analytics/Market_Analysis/Anti-Fraud?ysclid=mgtsbds8hl137030979) (дата обращения 10.09.2025).

платформы «Гостех» до марта 2026 года). Однако необходимым условием успешной работы в этом направлении видится не только господдержка таких разработок, но и возможность реализации компетенций сотрудниками правоохранительных органов, позволяющих понимать специфику функционирования киберсферы, её трансграничный характер, умение работать в информационной среде, коммуницировать с представителями IT-компаний и другими специалистами.

**ПИЧУГИН Сергей Анатольевич**

кандидат юридических наук, доцент

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

доцент кафедры криминалистики

**[pichugin81@mail.ru](mailto:pichugin81@mail.ru)**

125993, Россия, г. Москва, ул. Садовая-Кудринская, 9

## МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ АНТРОПОЛОГИЧЕСКОГО ПОДХОДА В ПОРТРЕТНОЙ ИДЕНТИФИКАЦИИ

**Аннотация.** В контексте глобализации, характеризующейся беспрецедентным ростом мобильности населения и формированием поликультурных сообществ, перед криминалистикой остро встает проблема адекватной идентификации личности. В данной статье обосновывается актуальность и необходимость интеграции антропологического подхода в существующую криминалистическую практику. Эмпирические данные свидетельствуют о том, что традиционные методы криминалистической габитоскопии, сформированные в рамках евроцентричной научной парадигмы и ориентированные преимущественно на европеоидный морфотип, демонстрируют системную недостаточность при работе с лицами иной этно-антропологической принадлежности. Это приводит к снижению точности и надежности идентификации, что, в свою очередь, ставит под сомнение эффективность правоохранительной деятельности в мультикультурной среде.

В качестве альтернативной методологической базы в исследовании предлагается использовать аппарат этнической антропологии, который акцентирует внимание на устойчивости ключевых фенотипических признаков (таких как лицевые параметры, пигментация кожного и волосяного покрова, радужной оболочки, особенности строения черепа и мягких тканей) на протяжении жизни индивида. Эти признаки, обладающие высокой консервативностью, представляют особую ценность для целей идентификации.

Центральной задачей статьи является проведение сравнительного анализа двух фундаментальных методологических концепций исследования признаков внешности человека — типологической и популяционной — для оценки их теоретического потенциала и практической применимости в криминалистике. В исследовании был использован комплексный методический аппарат, включающий эмпирическое сравнение антропологических данных, инструментарий криминалистической габитоскопии (включая видеотехнические и фотопортретные методы), классическую антропометрию, а также методы

этнической антропологии и расоведения, направленные на изучение варибельности признаков в популяциях.

В результате проведенного анализа было установлено, что типологическая концепция, основанная на выделении дискретных «чистых» антропологических типов, обладает ограниченной применимостью в современной криминалистической практике. Её основной недостаток проявляется при исследовании родственников, чьи признаки варьируются в рамках наследственности, и, что особенно важно, лиц смешанного происхождения, фенотип которых не укладывается в рамки жёстких типологических схем.

В качестве более релевантной и эффективной методологической основы в статье предлагается популяционный подход. Данный подход фокусируется не на поиске «идеальных» типов, а на анализе групповой изменчивости и непрерывности (континуальности) развития фенотипических характеристик внутри конкретных антропологических популяций. Такой взгляд позволяет строить более гибкие и точные идентификационные модели, учитывающие реальное разнообразие человеческих черт. Таким образом, интеграция популяционного подхода в практику криминалистической габитоскопии открывает новые возможности для повышения эффективности идентификации личности в условиях антропологического разнообразия современного мира.

**Ключевые слова:** антропологический подход, судебная портретная экспертиза, криминалистическая габитоскопия, этническая антропология, адаптивный тип, фенотипические признаки, обобщенный портрет, морфологические признаки, популяционная изменчивость.

S.A. PICHUGIN,  
Candidate of Law, Associate Professor,  
Kutafin Moscow State Law University (MSAL),  
Associate Professor of the Department of Criminalistics,  
pichugin81@mail.ru  
9 Sadovaya-Kudrinskaya Str., Moscow, 125993, Russia

#### **METHODOLOGICAL FOUNDATIONS OF THE USE OF THE ANTHROPOLOGICAL APPROACH IN PORTRAIT IDENTIFICATION**

**Annotation.** In the context of globalization, characterized by an unprecedented increase in population mobility and the formation of multicultural communities, criminology is faced with an acute problem of adequate identification. This article substantiates the relevance and necessity of integrating the anthropological approach into existing forensic practice. Empirical evidence suggests that traditional methods of forensic habitoscopy, formed within the framework of a eurocentric scientific paradigm and focused primarily on the Caucasoid morphotype, demonstrate systemic insufficiency when working with people of a different ethno-anthropological background. This leads to a decrease in the accuracy and reliability of identification, which, in turn, calls into question the effectiveness of law enforcement in a multicultural environment. As an alternative methodological base in the study, it is proposed to use the apparatus of ethnic anthropology, which focuses on the stability of key phenotypic features (such as facial parameters, pigmentation of skin and hair,

*iris, features of the skull and soft tissue structure) throughout an individual's life. These features, being highly conservative, are of particular value for identification purposes. The central objective of the article is to conduct a comparative analysis of two fundamental methodological concepts for the study of human appearance features — typological and population-based — to assess their theoretical potential and practical applicability in criminology. The study used a comprehensive methodological apparatus, including empirical comparison of anthropological data, tools of forensic habitoscopy (including video and photographic portrait methods), classical anthropometry, as well as methods of ethnic anthropology and racial studies aimed at studying the variability of traits in populations. As a result of the analysis, it was found that the typological concept based on the identification of discrete «pure» anthropological types has limited applicability in modern forensic practice. Its main disadvantage is manifested in the study of relatives, whose characteristics vary within the framework of heredity, and, most importantly, people of mixed origin, whose phenotype does not fit into the framework of strict typological schemes. The article suggests a population-based approach as a more relevant and effective methodological framework. This approach focuses not on the search for «ideal» types, but on the analysis of group variability and the continuity of the development of phenotypic characteristics within specific anthropological populations. This view allows us to build more flexible and accurate identification models that take into account the real diversity of human traits. Thus, the integration of the population approach into the practice of forensic habitoscopy opens up new opportunities for improving the effectiveness of personal identification in the context of the anthropological diversity of the modern world.*

**Key words:** *anthropological approach, forensic portrait examination, criminalistic habitoscopy, ethnic anthropology, adaptive type, phenotypic features, generalized portrait, morphological features, population variability.*

В условиях глобализации и увеличения миграционной мобильности современная криминалистика и судебная экспертиза сталкиваются с необходимостью идентификации лиц, принадлежащих к различным антропологическим типам. Классические методики габитоскопии, разработанные преимущественно на основе европеоидных фенотипов, зачастую оказываются недостаточно эффективными при работе с неевропеоидными чертами внешности. Это обуславливает растущую значимость антропологического подхода, который становится не просто дополнением, а ключевым элементом, перестраивающим саму методологию портретных экспертиз и составления субъективных портретов.

Интеграция антропологических знаний в автоматизированные системы, такие как регистрационно-поисковая система «Портрет-Поиск вер. 5.0», позволяет систематизировать и фиксировать внешние признаки с учетом этнической и популяционной специфики. Этот подход обеспечивает не только генерацию признаков внешности, но и создание визуально-реалистичных образов представителей различных этносов. Его применение критически важно для опознания лиц по фото- и

видеоизображениям, особенно в сложных случаях, связанных с возрастными трансформациями, действиями пластической хирургии или намеренной маскировкой.

Методологическим стержнем применения антропологического подхода в экспертизе выступает концепция этнической антропологии, изучающая вариативность признаков человеческих популяций. Современная наука рассматривает человечество как единый биологический вид *Homo sapiens*, внутри которого исторически сложились системные подразделения — расы. Как подчеркивал Я.Я. Рогинский, расы представляют собой не дискретные типы, а исторически сложившиеся системы популяций, характеризующиеся комплексом наследственных биологических признаков, сформировавшихся в определенных географических ареалах<sup>1</sup>.

Процесс формирования этих признаков детерминирован генетической изоляцией. По мнению И.В. Перевозчикова, длительная изоляция популяций приводит к накоплению различий в генофонде и, как следствие, во внешних физических характеристиках (фенофонде)<sup>2</sup>. В данном контексте раса понимается исключительно как биологическая категория, описывающая группу людей с комплексом наследуемых физических маркеров (антропометрические параметры, цвет и тип волос, строение мягких тканей лица, пигментация кожи и др.), используемых для идентификации личности.

Ключевые фенотипические характеристики, определяющие строение крупных антропологических групп (европеоидной, монголоидной, негроидной), отличаются высокой устойчивостью. Такие особенности, как параметры лицевого скелета, пигментация, форма носа и губ, сохраняются на протяжении жизни индивида. Однако, как справедливо отмечал Я.Я. Рогинский, не все физические параметры являются расообразующими. Признаки телосложения, развитие мускулатуры и жировой ткани сильно варьируются под влиянием среды, питания и образа жизни, а потому не служат надёжными диагностическими маркерами<sup>3</sup>.

---

<sup>1</sup> См.: Рогинский, Я.Я. Антропология: учебник / Я.Я. Рогинский, М.Г. Левин. — 3-е изд., испр. и доп. Москва: Высшая школа, 1978. — 528 с.

<sup>2</sup> Перевозчиков, И.В. Изменчивость расовых признаков внешности человека / И.В. Перевозчиков // Вестник Московского университета МВД России. — 2013. — № 4. — С. 8.

<sup>3</sup> Рогинский, Я.Я. Указ. соч. — 528 с.

Уникальность внешности индивида детерминирована генетически. Наследственно закреплённые антропологические признаки окончательно формируются к периоду физиологической зрелости (около 25 лет), но и в дальнейшем не остаются абсолютно статичными, претерпевая наиболее заметные изменения при переходе от зрелого к пожилому возрасту.

Внешний облик человека как продукт эволюции демонстрирует устойчивость ключевых морфологических параметров к прямому влиянию среды. Антрополог Т.И. Алексеева указывала, что процессы роста и формообразования фенотипических признаков представляют собой сложный комплекс метаболических механизмов, в значительной степени генетически детерминированных. Однако их развитие неразрывно связано с географическим контекстом, что нашло отражение в теории «адаптивного типа». Согласно Т.И. Алексеевой, адаптивный тип — это биологическая норма реакции на комплекс условий среды, обеспечивающая популяционное равновесие и находящая выражение в специфике внешности<sup>1</sup>.

Наличие у индивида морфологических черт, нетипичных для основной популяции региона, может служить индикатором его миграционного происхождения. Степень выраженности этих антропологических маркеров позволяет косвенно оценить длительность пребывания человека на новой территории, а привлечение специалиста даёт возможность с определённой вероятностью реконструировать вероятный географический источник миграции.

Методология начинается с детальной фиксации и описания дискретных признаков (общая величина носа, высота и ширина лица, форма глазной щели, профилировка губ и т.д.), которые интерпретируются как фенотипические адаптации. Последующее картографирование ареалов распространения таких черт предоставляет объективный инструмент для сравнительного анализа. Данные геномных исследований окончательно подтверждают, что фенотипические вариации являются поверхностными адаптациями к локальным условиям среды и не свидетельствуют о глубоких генетических различиях между группами.

Кроме того, внешний облик индивида формируется под мощным воздействием социокультурного контекста. Такие элементы, как

---

<sup>1</sup> Алексеева, Т.И. *Адаптация человека в различных экологических нишах Земли (Биол. аспекты): Курс лекций / Т.И. Алексеева; Междунар. независимый экол.-политол. ун-т. — Москва: Изд-во МНЭПУ, 1998. — 278 с.*

причёска, борода и усы, одежда, головные уборы, украшения (например, лабретки, серьги, расширяющие мочку уха) или практики искусственной деформации черепа и шеи, способны значительно трансформировать морфологическое восприятие. В процессе анализа криминалисту необходимо учитывать эту обусловленность и избегать трактовки подобных признаков как сугубо наследственных.

В рамках криминалистической габитоскопии под признаками внешности понимаются любые видимые характеристики, позволяющие дифференцировать как этно-территориальные группы, так и конкретных индивидов. При работе с неевропейскими фенотипами ключевое значение приобретает не уникальность отдельного признака, а его идентификационная значимость в комплексе с другими.

Для анализа закономерностей изменчивости внешности используются два основных подхода:

1. Типологический подход. Основан на концепции комплексного наследования антропологических характеристик, передающихся в виде устойчивых групп признаков. Данный метод предполагает выделение «чистых» антропологических типов, а задача специалиста заключается в оценке степени соответствия индивида тому или иному идеализированному эталону. Теоретически это позволяет количественно оценить антропологическую принадлежность. Главный недостаток — постулат о статичности «расовых» свойств, игнорирующий естественную вариабельность и смешение популяций. На практике выделение «чистых» признаков проблематично, что может привести к ошибочным выводам. Например, при сравнении внешности близких родственников эксперт, опираясь на этот метод, может ошибочно отнести их к разным антропологическим группам из-за субъективной интерпретации различающихся комплексов признаков.

2. Популяционный подход. Определяет антропологический тип не как совокупность черт индивида, а как комплекс фенотипических признаков, свойственных крупным группам популяций. Этот подход акцентирует внимание на групповой изменчивости и генетической близости. Первичным элементом здесь считается исторически сложившаяся популяция с уникальной фенотипической структурой. Ключевым аспектом является понимание того, что фенотипические признаки наследуются не как жёстко связанный комплекс, а независимо, образуя вариативные сочетания. Границы между антропологическими типами в рамках этого подхода оказываются размытыми и условными.

Оба подхода, предоставляя теоретическую базу, не позволяют визуализировать эталонный тип для решения практических задач. Для формулирования объективного вывода возникает необходимость в построении обобщённого портрета.

Обобщённый портрет — это идеализированная конструкция, базирующаяся на статистически доминирующих морфологических чертах, свойственных группе людей, объединённых общим ареалом и генетическим фоном. Его создание требует масштабных инструментальных исследований (фотограмметрия, 3D-сканирование) и последующей статистической обработки данных для выявления модальных (наиболее частых) значений. Принципы метода интегрируются в алгоритмы поисковых систем и нейросетей для автоматизированного распознавания и верификации личности. В современной габитоскопии метод развивается в сторону анализа не только статичных, но и динамических признаков (мимика, артикуляция, походка), которые также имеют популяционную специфику.

Современная портретная идентификация, основанная на глубоком понимании популяционных закономерностей, выходит на новый уровень. Её перспективы напрямую связаны с междисциплинарной конвергенцией и внедрением цифровых технологий.

Ключевые стратегические векторы развития включают:

1. Развитие 3D-моделирования и математических методов. Создание трехмерных анатомически точных моделей головы и внедрение алгоритмов для статистического анализа морфологии позволят минимизировать субъективный фактор и проводить более точные антропометрические измерения.

2. Формирование унифицированных этно-антропологических баз данных. Создание и стандартизация регистрационно-поисковых систем, систематизирующих антропометрические данные для различных этнических и популяционных групп, является основой для сравнительного анализа.

3. Автоматизация процессов анализа. Разработка специализированного программного обеспечения для автономного анализа изображений с использованием компьютерных средств для выделения и классификации диагностически значимых признаков<sup>1</sup>.

---

<sup>1</sup> См.: Сидорова, К.С. IP-адрес как один из идентификаторов личности в расследовании преступлений / К.С. Сидорова // Психопедагогика в правоохранительных органах. — 2018. — № 3(74). — С. 84-87.

Необходимость системного применения антропологического подхода в современной экспертной практике продиктована объективными вызовами глобализированного мира. Задачи идентификации лиц с существенными отклонениями от среднеевропейских фенотипических параметров требуют от специалиста глубоких знаний в области популяционной антропологии, адаптологии и современных цифровых технологий. Понимание того, что морфологические признаки являются продуктом сложного взаимодействия генетики, адаптации и культуры, позволяет не только эффективно осуществлять портретную идентификацию в сложных политипичных условиях, но и выводить всю сферу портретной экспертизы на качественно новый, научно обоснованный уровень. Антропометрический подход, синтезирующий принципы криминалистики и антропологии, формирует высокоэффективный инструментарий, который становится стратегическим ресурсом в обеспечении правопорядка.

#### БИБЛИОГРАФИЯ:

1. *Алексеева, Т.И. Адаптация человека в различных экологических нишах Земли (Биол. аспекты): Курс лекций. Междунар. независимый экол.-политол. ун-т. — Москва: Изд-во МНЭПУ, 1998. — 278 с.*
2. *Перевозчиков, И.В. Изменчивость расовых признаков внешности человека // Вестник Московского университета МВД России. — 2013. — № 4. — С. 8.*
3. *Рогинский, Я.Я., Левин, М.Г. Антропология: учебник. — 3-е изд., испр. и доп. — Москва: Высшая школа, 1978. — 528 с.*
4. *Сидорова, К.С. IP-адрес как один из идентификаторов личности в расследовании преступлений // Психопедагогика в правоохранительных органах. — 2018. — № 3(74). — С. 84-87.*

**Трибуна молодых ученых**

УДК 343.9  
ББК 67.523.12

**ГОЛОЛОБОВ Леонид Сергеевич**

*Московский государственный юридический университет имени О.Е. Кутафина (МГЮА),  
обучающийся Института публичного права и управления*

***g.obla@bk.ru***

*125993, Россия, г. Москва, ул. Садовая-Кудринская, 9*

**НАУЧНЫЙ РУКОВОДИТЕЛЬ:**

**КОМИССАРОВА Ярослава Владимировна**

*кандидат юридических наук, доцент,  
почетный работник сферы образования Российской Федерации*

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

*доцент кафедры криминалистики (с возложением обязанностей заместителя заведующего кафедрой по научной работе)*

*главный редактор федерального научно-практического журнала  
«Эксперт-криминалист»*

***a5143836@yandex.ru***

*125993, Россия, г. Москва, ул. Садовая-Кудринская, 9*

---

**НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ  
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В КРИМИНАЛИСТИКЕ**

**Аннотация.** В статье затрагиваются вопросы использования новых технологий в криминалистике, в частности, технологий искусственного интеллекта, которые окажут значительное влияние на процесс расследования преступлений, облегчат сотрудникам правоохранительных органов работу по добыванию доказательств. Выполнен анализ некоторых существующих программ, дана оценка их эффективности. Исследованы отдельные проблемы внедрения новых технологий в практику противодействия преступности.

**Ключевые слова:** борьба с преступностью, криминалистика, информационно-коммуникационные технологии, искусственный интеллект, автоматизированные информационные системы.

L.S. GOLOLOBOV,  
Kutafin Moscow State Law University (MSAL),  
Student at the Institute of Public Law and Administration  
g.obla@bk.ru  
9 Sadovaya-Kudrinskaya Str., Moscow, 125993, Russia

SCIENTIFIC SUPERVISOR:  
YA. V. KOMISSAROVA,  
Candidate of Law, Associate Professor,  
Honorary Worker of Education of the Russian Federation,  
Kutafin Moscow State Law University (MSAL),  
Associate Professor of the Department of Criminalistics  
(with the duties of Deputy Head of the Department for Research),  
Editor-in-Chief of the Federal Scientific and Practical Journal «Forensics  
analyst», Candidate of Legal Sciences, Associate Professor,  
a5143836@yandex.ru  
9 Sadovaya-Kudrinskaya Str., Moscow, 125993, Russia

#### **SOME ASPECTS OF THE USE OF MODERN INFORMATION TECHNOLOGIES IN FORENSIC SCIENCE**

**Annotation.** *The article discusses the use of new technologies in criminology, in particular, artificial intelligence technologies, which will have a significant impact on the process of investigating crimes and will make it easier for law enforcement officers to obtain evidence. An analysis of some existing programs has been performed, and an assessment of their effectiveness has been given. The individual problems of introducing new technologies into the practice of combating crime are investigated.*

**Key words:** *crime prevention, criminalistics, information and communication technologies, artificial intelligence, automated information systems.*

Введение. В настоящее время в связи с развитием информационно-коммуникационных технологий преступники их активно осваивают и часто используют для достижения противоправных целей. Соответственно, особое значение приобретает использование данных технологий в деятельности правоохранительных органов, ускорение внедрения их в практику борьбы с преступностью.

Так, по данным МВД России за 2023 год зарегистрированы 677 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 29,7 % больше, чем в 2022 году. В общем числе зарегистрированных преступлений в сравнении с 2022 годом их удельный

вес увеличился с 26,5 % до 34,8 %<sup>1</sup>. В 2024 году 40 % из общего числа преступлений были совершены с использованием информационно-телекоммуникационных технологий. Таких деяний зарегистрировано на 13,1 % больше, чем в 2023 году. В значительной степени этот фактор повлиял на рост в 2024 году общего числа тяжких и особо тяжких преступлений на 4,8%<sup>2</sup>.

Это свидетельствует о росте угрозы обществу со стороны преступности, использующей достижения науки в противоправных целях. Поэтому важным и злободневным вопросом сегодняшней повестки является изучение возможности использования информационных технологий в борьбе с преступностью, прежде всего, при раскрытии и расследовании преступлений.

Криминалистика призвана обеспечивать быстрое и качественное расследование преступлений. Несомненно, методы, ею выработанные, основаны на фундаментальных положениях науки, однако некоторые, особенно технико-криминалистические, значительно отстают от требований современности. Сегодня востребованы новые инструменты для борьбы с преступностью. Поэтому, как справедливо отмечает В.В. Колиев, современная криминалистика идёт по пути «разработки и помощи в освоении программного обеспечения, направленного на обнаружение, изъятие и исследование доказательственной информации, упрощения проведения отдельных следственных действий»<sup>3</sup>.

*Использование камер видеонаблюдения с возможностью распознавания лиц* — первое, на что следует обратить внимание.

Распоряжением Правительства Российской Федерации от 03.12.2014 № 2446-р «Об утверждении Концепции построения и развития аппаратно-программного комплекса "Безопасный город"»<sup>4</sup> было

---

<sup>1</sup> Состояние преступности в России за январь-декабрь 2023 года. — [Электронный ресурс]. — Режим доступа: — URL: <https://portal.tpu.ru/> (дата обращения 02.10.2025).

<sup>2</sup> Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2024 года — [Электронный ресурс]. — Режим доступа: — URL: <https://мвд.рф/reports/item/60248328/> (дата обращения 02.10.2025).

<sup>3</sup> Колиев, В. В. Инновационное развитие криминалистики / В.В. Колиев // Право и государство: теория и практика. — 2023. — № 4 (220). — [Электронный ресурс]. — Режим доступа: — URL: <https://cyberleninka.ru/article/n/innovatsionnoe-razvitiie-kriminalistiki> (дата обращения: 09.09.2025).

<sup>4</sup> Распоряжение Правительства Российской Федерации от 03.12.2014 № 2446-р «Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» // Собрание законодательства РФ. — 2014. — № 50. — Ст. 7220.

предусмотрено развитие новой технологии для повышения уровня общественной безопасности, обеспечения правопорядка и безопасности граждан. Предусматривалось оснащение городов и других муниципальных образований системами камер видеонаблюдения, включая возможность распознавания лиц; создание единой информационной базы, видео- и аудиоархива; системы оповещения о совершаемых преступлениях.

Сегодня при наличии фотографии предполагаемого преступника или его фотокомпозиционного портрета имеется возможность загрузки данного изображения в систему «Безопасный город», которая при фиксации похожего лица подает сигнал оповещения (указывается вероятность идентификации в процентном соотношении). То есть фактически, если подозреваемый попадает в поле зрения видеокамер, система предоставляет информацию о том, где это произошло и насколько внешность субъекта совпадает с загруженным изображением.

Данная система эффективно используется в Москве, Санкт-Петербурге, Московской области и ряде крупных городов некоторых регионов Российской Федерации.

Например, в г. Москве в проекте «Безопасный город» применяется две системы: на объектах общественного назначения и подъездах жилых домов — подсистема автоматической регистрации сценариев индексирования видеоинформации «Единого центра хранения и обработки данных» (ПАРСИВ), на объектах транспорта (метро, вокзалы, переходы и т.д.) — государственная автоматизированная информационная система «Сфера» (ГАИС «Сфера»).

Министр цифрового развития, связи и массовых коммуникаций Российской Федерации М.И. Шадяев отметил, что за 10 лет, которые прошли с момента развития системы «Безопасный город» в Москве, количество зарегистрированных преступлений (так называемой «уличной преступности») уменьшилось в два раза, угонов автотранспорта — в 10 раз, а раскрываемость тех преступлений, которые продолжают фиксироваться, выросла в два раза<sup>1</sup>.

Несмотря на это, в использовании данной системы имеются и недостатки, над устранением которых нужно еще поработать. В частности, в Российской Федерации нет закона, обязывающего не

---

<sup>1</sup> В России треть камер «Безопасного города» подключены к системе распознавания лиц. — [Электронный ресурс]. — Режим доступа: — URL: <https://www.interfax.ru/russia/950126> (дата обращения 12.05.2024).

закрывать полностью лицо без каких-либо к тому медицинских показаний, что значительно затрудняет процесс распознавания. Проблема обострилась в период пандемии коронавируса Covid-19, когда ношение медицинских масок стало частью повседневной жизни. Маска в совокупности с надетым головным убором и солнечными очками практически не позволяет системе распознавания лиц сработать, что аналогично ношению преступниками балаклавы, скрывающей лицо.

В связи с этим встал вопрос об использовании технологий искусственного интеллекта (далее — ИИ) применительно к АПК «Безопасный город» — о распознавании силуэта, походки человека, поведенческих актов и других индивидуальных признаков, не связанных с лицом человека<sup>1</sup>.

Примеры использования указанных сведений о человеке уже имеются в зарубежной практике. Так, китайские ученые представили программу, которая распознает силуэт и походку человека<sup>2</sup>. Основываясь на данных видеонаблюдения, система сопоставляет силуэт с общей базой данных и находит совпадение. «Перехитрить» систему вряд ли получится, так как походка каждого человека уникальна.

Учитывая то, что в некоторых регионах России похожая технология уже прошла тестирование, в скором времени возможно ее повсеместное применение. Так, в г. Томске в 2022 году протестировали систему «Визирь», которая может распознавать людей в капюшонах, очках, масках. Власти планируют внедрить данную систему в регионе, так как результаты тестирования признаны удовлетворительными<sup>3</sup>. Система видеоидентификации «Визирь» показала свою эффективность «в условиях плотного потока людей на объектах транспорта, спорта и в местах массового пребывания людей»<sup>4</sup>.

---

<sup>1</sup> См., например: Манухова, К.В. Габитоскопия в эпоху цифровых технологий: интеграция с АПК «Безопасный город» / К.В. Манухова, Н.А. Костикова // Эксперт-криминалист. — 2025. — № 4. — С. 25-28.

<sup>2</sup> Китайских нарушителей выследят по походке. — [Электронный ресурс]. — Режим доступа: — URL: [https://lenta.ru/news/2018/11/08/uznayu\\_po\\_pohodke/](https://lenta.ru/news/2018/11/08/uznayu_po_pohodke/) (дата обращения 02.10.2025).

<sup>3</sup> Систему распознавания людей по силуэтам хотят внедрить в Томской области. — [Электронный ресурс]. — Режим доступа: — URL: <https://news.vtomske.ru/news/187368-sistemu-raspoznavaniya-lyudei-po-siluetam-hotyat-vnedrit-v-tomskoi-oblasti> (дата обращения 03.10.2025).

<sup>4</sup> Автоматизированная система видеоидентификации физических лиц «Визирь», презентация проекта. — [Электронный ресурс]. — Режим доступа: — URL: <https://digital.mosreg.ru/ai-solutions/173> (дата обращения: 02.10.2025).

Как нам представляется, в рамках работы АПК «Безопасный город» существует возможность идентификации похищенного имущества. Например, при краже женской сумочки или чемодана (при наличии их изображения) можно отслеживать похожие предметы по камерам видеонаблюдения, что в конечном итоге позволит установить лицо, совершившее преступление, или его сообщников. Внедрение такого технического решения в практику повысит результативность процесса раскрытия преступлений, его длительность сократится, что увеличит эффективность правоохранительной деятельности в целом.

*Возможность выявления серийных преступлений* — второе, чем современные информационно-коммуникационные технологии могут помочь криминалистике.

Необходимо отметить, что современная преступность характеризуется широким региональным охватом. То есть лицо, совершающее одни и те же преступления одинаковым способом с использованием аналогичных средств («почерк» преступника), может беспрепятственно и без каких-либо затруднений перемещаться по стране. Транспортная доступность и большие миграционные потоки этому способствуют. Соответственно, если между правоохранительными органами нет эффективного взаимодействия и по неочевидному преступлению не отрабатывается версия о межрегиональном характере действий преступника (так называемом «гастролере»), с большой долей вероятности можно предположить, что оно останется нераскрытым.

Здесь, по нашему мнению, помощь как раз и могут оказать современные информационные технологии. Так как ИИ поддается различным вариантам обучения, представляется, что есть возможность его использования для распознавания признаков серийности нераскрытых преступлений. Для этого необходимо научить ИИ находить общие признаки совершенных противоправных деяний и выдавать результаты в удобной для правоохранительных органов форме. Конечно, важно, чтобы все особенности преступления, выявленные криминалистами, вносились в соответствующую базу данных, так как без достоверных исходных сведений эффективно использовать технологию будет проблематично.

Подобные исследования на примере практики раскрытия серийных убийств уже проводились, что позволило А.А. Бессонову прийти к выводу, что при обучении ИИ удастся достигнуть высокой степени точности прогнозирования признаков неизвестного серийного преступника. Предполагается, что эта система позволит реализовывать два алгоритма

расследования: 1) «от вероятностного портрета преступника — к еще не обнаруженным следам преступления»; 2) «от вероятностного портрета преступника — к конкретному подозреваемому».

В настоящее время указанный выше алгоритм уже используется Главным управлением криминалистики (Криминалистическим центром) Следственного комитета Российской Федерации<sup>1</sup>. Однако, как представляется, развивать идею можно и нужно применительно ко всем аспектам борьбы с преступностью, а не только по делам о преступлениях против личности. Это позволит повысить раскрываемость таких наиболее распространенных преступлений, как мошенничества и грабежи, которые давно вышли за пределы территории одного субъекта и могут совершаться по всей России одними и теми же лицами.

*Использование иных технологий искусственного интеллекта.* В целом в России активно используются возможности ИИ в сфере борьбы с преступностью. Так, в нашей стране разработана система «Криминалист», которая позволяет анализировать данные из разных источников, таких как базы данных правоохранительных и иных органов исполнительной власти (МВД, ФСБ, ФНС России, Росфинмониторинга и других), а также из открытых источников (сведения из средств массовой информации, социальных сетей, интернет-источников). Система «Криминалист» помогает обнаруживать потенциальных преступников, места совершения преступлений, а также предлагать оптимальные решения для правоохранителей. Используются и иные автоматизированные информационно-поисковые системы с внедренными алгоритмами ИИ, позволяющие получать информацию о возможных направлениях расследования: «Блок» — криминалистическое сопровождение расследования экономических преступлений, «Сейф» — информация о хищениях денежных средств из хранилищ; «Спрут» — установление контактных связей преступников и т.д.

Также посредством применения ИИ можно воссоздавать обстановку на месте совершения преступления и анализировать детали преступного события, даже если изначально что-то было упущено из виду. Автоматическое объёмное моделирование обстановки места преступления (места происшествия) в процессе производства судебных

---

<sup>1</sup> Бессонов, А.А. Использование алгоритмов искусственного интеллекта в криминалистическом изучении преступной деятельности (на примере серийных преступлений) / А.А. Бессонов // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2021. — № 2. — С. 53.

экспертиз позволит свести к минимуму ошибки, допускаемые из-за так называемого «человеческого фактора»<sup>1</sup>.

В мировой практике имеется опыт использования таких систем, как PredPol (Predictive Policing), которая прогнозирует вероятность совершения преступлений в определённых местах в определённый промежуток времени на основе анализа накопленных данных о правонарушениях; алгоритма COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), оценивающего риск рецидива у осужденных и подсудимых на основе анализа разных факторов; программы ShotSpotter, обнаруживающей выстрелы из огнестрельного оружия и определяющей место происшествия<sup>2</sup>.

Проблемные аспекты использования ИИ. Как мы видим, внедрение технологий ИИ в процесс раскрытия и расследования преступлений имеет большой потенциал. Вместе с тем, в настоящее время есть и проблемы, возникающие в деятельности правоохранительных органов, нерешенность которых влияет на использование ИИ в борьбе с преступностью:

1. Устаревшая криминалистическая техника, используемая криминалистами и другими сотрудниками правоохранительных органов в некоторых отдаленных регионах России.

2. Отсутствие АПК «Безопасный город» в небольших городах и малых населенных пунктах. Хотя программа освоения данной системы подразумевает ее распространение на территории всей Российской Федерации до 2030 года, в основном это касается только региональных центров. Когда данная возможность появится в других территориальных образованиях, пока неизвестно.

3. Отсутствие доступа ко всем федеральным учетам и информационным массивам, в которых используется ИИ и их разноплатформенность. За пределами Москвы еще только предстоит обеспечить соответствующий доступ всем криминалистам, являющимся сотрудниками правоохранительных органов, к таким системам. Эту сложную задачу усугубляет и то, что различные системы, использующие возможности ИИ, созданы на неоднородных платформах (в разных

---

<sup>1</sup> Пинчук, П.В. О применении трехмерного моделирования в рамках проведения комплексной судебно-медицинской и автотехнической экспертизы / П.В. Пинчук, С.В. Леонов, О.Ю. Самаркина // Эксперт-криминалист. — 2023. — № 2. — С. 35–37.

<sup>2</sup> Нейронное дело: как ИИ помогает в борьбе с преступностью. — [Электронный ресурс]. — Режим доступа: — URL: <https://iz.ru/1569903/alena-svetunkova/neironnoe-delo-kak-ii-pomogaet-v-borbe-s-prestupnosti> (дата обращения 13.09.2025).

операционных системах, программных средствах и т.п.), имеющих свои характерные особенности, усложняющие процедуру их применения.

4. Нехватка специалистов, осваивающих ИИ, способных применять его в процессе раскрытия и расследования преступлений. Так называемый «кадровый голод», имеющийся в системе МВД России, а также неразвитость профессионального повышения квалификации сотрудников по работе с ИИ, затормаживают процесс освоения новых технологий.

5. Организационные и технические проблемы, связанные как с нехваткой финансирования, так и с непониманием важности использования и применения новых информационных технологий.

**Заключение.** Решение указанных выше и иных проблем видится в программном документе единого характера (например, Постановление Правительства Российской Федерации), устраняющем все правовые и организационные коллизии, позволяющем без лишних бюрократических процедур наиболее быстро и эффективно осваивать новые технико-криминалистические методы работы на основе ИИ. Так как это, прежде всего, вопросы повышения безопасности общества, они должны разрешаться без каких-либо проволочек. Только в таком случае будет обеспечено успешное противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий. Если передовые технологии будут осваиваться правоохранительными органами своевременно, удастся достичь существенных прорывных результатов в борьбе с преступностью.

#### **БИБЛИОГРАФИЯ:**

1. *Бессонов, А.А.* Использование алгоритмов искусственного интеллекта в криминалистическом изучении преступной деятельности (на примере серийных преступлений) // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2021. — № 2. — С. 45-53.

2. *Колиев, В. В.* Инновационное развитие криминалистики // Право и государство: теория и практика. — 2023. — № 4 (220). — [Электронный ресурс]. — Режим доступа: — URL: <https://cyberleninka.ru/article/n/innovatsionnoe-razvitie-kriminalistiki> (дата обращения: 09.09.2025).

3. *Манухова, К.В., Костинова, Н.А.* Габитоскопия в эпоху цифровых технологий: интеграция с АПК «Безопасный город» // Эксперт-криминалист. — 2025. — № 4. — С. 25-28.

**КАРАГОДИНА Камилла Евгеньевна**

Московский государственный юридический университет имени О.Е. Кутафина (МГЮА),  
обучающаяся Института судебных экспертиз

**s2011816@edu.msal.ru**

125993, Россия, г. Москва, ул. Садовая-Кудринская, 9

НАУЧНЫЙ РУКОВОДИТЕЛЬ:

**БОГАТЫРЕВ Константин Михайлович**

кандидат юридических наук

Московский государственный юридический университет имени О.Е. Кутафина (МГЮА),  
старший преподаватель кафедры криминалистики

**kmbogatyrev@msal.ru**

125993, Россия, г. Москва, ул. Садовая-Кудринская, 9

---

**СОВЕРШЕНСТВОВАНИЕ ТЕХНИКО-КРИМИНАЛИСТИЧЕСКОГО  
ОБЕСПЕЧЕНИЯ РАССЛЕДОВАНИЯ ИТ-ПРЕСТУПЛЕНИЙ**

**Аннотация.** В статье рассматриваются актуальные проблемы совершенствования технико-криминалистического обеспечения расследования в сфере информационных технологий. Анализируются существующие методы и средства криминалистической техники, применяемые при расследовании таких преступлений. Особое внимание уделяется вопросам модернизации технического оснащения следственных подразделений, внедрению современных цифровых технологий и специализированного программного обеспечения. Исследуются проблемы подготовки специалистов в области цифровой криминалистики и пути их решения.

**Ключевые слова:** технико-криминалистическое обеспечение, ИТ-преступления, цифровая криминалистика, следственные действия, криминалистическая техника, расследование преступлений, информационные технологии, киберпреступность, цифровые следы.

K.E. KARAGODINA,  
Kutafin Moscow State Law University (MSAL),  
Student of Institute of Forensic Expertise  
s2011816@edu.msal.ru  
9 Sadovaya-Kudrinskaya Str., Moscow, 125993, Russia

SCIENTIFIC SUPERVISOR:  
K.M. Bogatyrev,  
Candidate of Law,  
Kutafin Moscow State Law University (MSAL),  
Senior lecturer of Criminalistics Department,  
kmbogatyrev@msal.ru  
9 Sadovaya-Kudrinskaya Str., Moscow, 125993, Russia

### **IMPROVEMENT OF TECHNICAL AND FORENSIC SUPPORT FOR THE INVESTIGATION OF IT CRIMES**

**Annotation.** *The article deals with the current problems of improving technical and forensic support for the investigation in IT. The existing methods and means of forensic technology used in the investigation of crimes in the field of information technology are analyzed. Special attention is paid to the modernization of technical equipment of investigative units, the introduction of modern digital technologies and specialized software. The problems of training specialists in the field of digital forensics and ways to solve them are being investigated.*

**Key words:** *technical and forensic support, IT crimes, digital forensics, investigative actions, forensic technology, crime investigation, information technologies, cybercrime, digital traces.*

В современных условиях развития информационных технологий особую актуальность приобретает именно проблема совершенствования технико-криминалистического обеспечения расследования преступлений в сфере информационных технологий. С одной стороны, цифровая трансформация общества создает множество аспектов, в которых возможно углубленное развитие человечества для приобретения абсолютно новых навыков, с другой — создает и новые возможности как для совершения преступлений, так и для их раскрытия и расследования.

Развитие цифровых технологий постоянно порождает новые способы совершения и сокрытия преступлений, а также ведет к изменению механизма их совершения. Особенно актуальной становится проблема борьбы с преступлениями в сфере информационно-коммуникационных технологий, поскольку с распространением мобильных устройств и иных средств цифровой электроники возникают новые формы правонарушений. Широкое распространение мобильных телефонов и смартфонов привело не только к появлению и

распространению вредоносных программ, специально созданных для таких устройств, но и к активному использованию таких устройств в контексте иных преступлений (в первую очередь — мошенничеств).

Кроме того, мобильные средства коммуникации все чаще используются для подготовки и совершения преступлений высокой степени общественной опасности (тяжких и особо тяжких) — осуществления террористических актов, взрывов, инициализации массовых беспорядков. Также с помощью мобильных устройств совершаются вымогательства, мошенничества различных видов и прочие противоправные действия, связанные с использованием современных технологий<sup>1</sup>. Такая ситуация делает борьбу с подобными преступлениями очень сложной, поскольку многие из них имеют экстерриториальный, транснациональный характер — преступники используют компьютерные сети, поддерживающие связи между странами и континентами. По этой причине вопросы противодействия таким преступлениям актуальны для всех государств независимо от их географического положения и уровня технологического развития.

Следует подчеркнуть, что большинство описанных преступлений выходят за пределы рамок, установленных гл. 28 Уголовного кодекса Российской Федерации («Преступления в сфере компьютерной информации»), регламентирующей ответственность за компьютерные преступления. В связи с этим в научной литературе и практике не раз предлагалось использовать термин «компьютерное преступление» не в юридическом, а в криминалистическом смысле<sup>2</sup>. Понятие «компьютерное преступление» в криминалистическом контексте должно обозначать совокупность преступлений, совершаемых с использованием компьютерных технологий, а также тех преступных деяний, в которых фигурируют информационные системы и средства коммуникации.

---

<sup>1</sup> *Милованова, М.М.* О способах мошенничества в сети «интернет» / М.М. Милованова, В.А. Шурухов // Имущественные отношения в Российской Федерации. — 2021. — № 10(241). — С. 86-87; *Милованова, М.М.* Проблемные аспекты изучения и установления личности кибермошенника / М.М. Милованова // Правовое обеспечение суверенитета России: проблемы и перспективы: Сборник докладов XXIV Международной научно-практической конференции и XXIV Международной научно-практической конференции Юридического факультета МГУ им. М.В. Ломоносова в рамках XIII Московской юридической недели. В 4-х частях, Москва, 21–24 ноября 2023 года. — Москва: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. — С. 294.

<sup>2</sup> *Халиуллин, А.И.* Подходы к определению компьютерной преступности // Проблемный анализ и государственно-управленческое проектирование. — 2011. — Т. 4, № 6. — С. 17.

По мнению Е.Р. Россинской и А.И. Семикаленовой, понятие «компьютерное преступление» в основном следует рассматривать в рамках криминалистической классификации, где оно включает в себя характерные признаки и методы совершения преступлений, а также механизмы их сокрытия и расследования. В этом контексте важна не столько формальная юридическая квалификация, сколько способ преступления, используемый злоумышленником, а также особенности его раскрытия и расследования. В криминалистическом анализе такие преступления обладают родовой характеристикой, включающей сведения о применяемых способах совершения преступлений, профилях преступников, потерпевших, обстоятельствах. Все это позволяет выработать более эффективные методы борьбы с подобного рода нарушениями, учитывающими современные особенности информационной среды<sup>1</sup>.

В то же время, при изучении преступлений, связанных с коммуникацией в цифровой медиасреде посредством социальных сетей («ВКонтакте», «Одноклассники» и др.), систем мгновенного обмена сообщениями (Telegram, WhatsApp, Viber) и иных ресурсов речь идет не столько о техническом, сколько о содержательном аспекте<sup>2</sup>. В связи с этим рассмотрение способа совершения «с использованием компьютерных технологий» в качестве основания для выделения группы «компьютерные преступления» представляется возможным, но не совсем удачным; предпочтительным видится выделение группы «преступления, совершаемые с использованием информационно-коммуникационных технологий», т.к. в названии находит отражение не только общность способа, но и специфика механизма таких преступлений.

Таким образом, развитие информационных технологий и мобильных коммуникаций делает необходимым постоянное совершенствование способов противодействия новым формам преступной деятельности, связанной с использованием цифровых средств и компьютерных систем. Важной задачей в этой сфере является не только нормативное урегулирование, но и развитие

---

<sup>1</sup> См.: Россинская, Е.Р., Семикаленова, А.И. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. — 2020. — № 3. — С. 745-759.

<sup>2</sup> См.: Галяшина, Е.И., Богатырев, К.М., Антонян, Е.А., Кокурин, А.В. Медиабезопасность в цифровой среде: роль сведущих лиц: монография. — Москва: Проспект, 2024. — 288 с.

криминалистической методики, которая учитывает особенности технологического характера преступлений, а также создание эффективных механизмов их обнаружения, расследования и пресечения.

IT-преступления характеризуются латентностью, обусловленной использованием технологий анонимизации (VPN, TOR, прокси-серверы), применением методов шифрования, а также возможностью совершения противоправных действий на межгосударственном уровне. Все это существенно усложняет работу правоохранительных органов и требует создания нового уровня технико-криминалистического обеспечения. Основными компонентами технико-криминалистического обеспечения расследования IT-преступлений являются: специальное оборудование для изъятия, копирования и анализа цифровых носителей информации, программное обеспечение, обеспечивающее автоматизированный поиск, обработку и систематизацию больших массивов данных, методы фиксации цифровых следов, позволяющие сохранить их процессуальную значимость, средства обеспечения информационной безопасности, предотвращающие утечку данных и несанкционированный доступ.

Исходя из вышесказанного, теоретическая база технико-криминалистического обеспечения опирается на междисциплинарный подход, объединяющий знания в области права, криминалистики и информационных технологий.

Современные средства, используемые в расследовании IT-преступлений, можно условно разделить на несколько групп: устройства для копирования и анализа данных с цифровых носителей (к ним относятся write-blocker'ы, предотвращающие изменение данных на носителе, и специализированные сканеры жестких дисков); специализированные комплексы для исследования мобильных устройств (например, UFED, XRY), позволяющие извлекать данные даже с заблокированных смартфонов; программное обеспечение для анализа сетевого трафика (Wireshark, NetworkMiner), позволяющее установить источники атак и выявить подозрительные соединения; системы восстановления удаленной информации, применяемые для возврата потерянных или намеренно уничтоженных данных; оборудование и программные средства для исследования криптографических систем и паролей. Применение данного перечня средств позволяет не только собирать цифровые доказательства, но и формировать целостную картину преступной деятельности.

Несмотря на наличие значительного числа технических решений, практика их применения выявляет ряд проблем. К примеру, быстрое

устаревание технических средств, так как развитие цифровых технологий делает оборудование морально устаревшим в течение 3-5 лет. Высокая стоимость современного оборудования также является некоторой границей, не позволяющей совершенствовать расследование в более короткий промежуток времени, это особенно актуально для региональных подразделений правоохранительных органов. Затруднения предоставляет и недостаточная подготовка специалистов, которые зачастую ограничены базовыми знаниями в области IT, что вполне вероятно скажется на понимании самой концепции действий, примененных преступным лицом в ходе совершения общественно-опасного деяния. Сложность интеграции различных технических средств — дополнительное препятствие, так как программные комплексы разных производителей не всегда совместимы. Более того, отсутствуют единые стандарты работы с доказательствами, имеющими цифровую форму представления, что ведет к риску признания их недопустимыми в суде.

При расследовании IT-преступлений необходимо строго соблюдать процессуальные правила обращения с цифровыми доказательствами. Прежде всего необходимо своевременно изъять цифровые носители, поскольку данные могут быть удалены или изменены в любой момент, немало важным является правильность упаковки и транспортировки, чтобы исключить возможность физического или программного воздействия. Необходимо соблюдать правила работы с электронными доказательствами, а именно использовать write-blocker'ы, создание копий и контрольных хэшей. Для детального описания проводимых следственных действий, а также для недопустимости утери важной информации, влияющей на раскрытие преступления, необходимо документирование всех этапов исследования в протоколах следственных действий, проводимых с привлечением обладающих компетенцией в области компьютерной техники лиц.

Совершенствование технической базы предполагает модернизацию с внедрением облачных технологий для хранения и обработки цифровых доказательств, использование искусственного интеллекта и машинного обучения для анализа больших массивов данных и выявления закономерностей, создание мобильных криминалистических комплексов, которые позволят оперативно реагировать на киберпреступления непосредственно на месте происшествия, разработку отечественного специализированного программного обеспечения, учитывающего правовые и технические особенности российского законодательства, обеспечение совместимости различных технических средств на основе

единых стандартов. Во-многом предложенный вариант действий уже был реализован при создании в русле ИИ-трансформации правоохранительных органов современной системы оперативно-розыскных мероприятий (СОПМ-3)<sup>1</sup>, а также иных технико-криминалистических средств (таких, как автоматизированные системы «Спрут», «Маньяк», «Криминалист» и т.д.)<sup>2</sup>.

Не менее важным направлением развития является подготовка кадров. Создание специализированных образовательных программ в вузах и академиях МВД и ФСБ России, организация регулярных курсов повышения квалификации для следователей и судебных экспертов, привлечение специалистов из частного IT-сектора, обладающих практическими навыками кибербезопасности, развитие системы стажировок в ведущих международных лабораториях цифровой криминалистики, активный обмен опытом с зарубежными коллегами — все приведенные выше методы способны усовершенствовать кадровый фактор, так как он напрямую определяет эффективность использования даже самых современных технических средств.

Совершенствование технико-криминалистического обеспечения расследования IT-преступлений безусловно должно носить комплексный характер. Оно должно включать: постоянное обновление технического оснащения, внедрение инновационных технологий (AI, Big Data), развитие кадрового потенциала, а также совершенствование методических и правовых основ. Таким образом, эффективное развитие данного направления позволит существенно повысить результативность борьбы с преступлениями рассмотренной группы, укрепить цифровую безопасность общества.

#### БИБЛИОГРАФИЯ:

1. *Галяшина, Е.И., Богатырев, К.М., Антонян, Е.А., Кокурин, А.В.* Медиабезопасность в цифровой среде: роль сведущих лиц: Монография. — М.: Проспект, 2024. — 288 с.
2. *Милованова, М.М., Шурухнов, В.А.* О способах мошенничества в сети «интернет» // Имущественные отношения в Российской Федерации. — 2021. — № 10(241). — С. 86-92.

---

<sup>1</sup> СОПМ 3 (как работает) // SecurityLab.ru [Электронный ресурс]. URL: <https://www.securitylab.ru/blog/personal/homoadminus/351753.php> (дата обращения: 28.09.2025).

<sup>2</sup> Технологии в праве, криминалистике и их влияние на преступность // Лигал Академия [Электронный ресурс]. URL: <https://legalacademy.ru/sphere/post/tehnologii-v-prave-kriminalistike-i-ih-vliyanii-na-prestupnost> (дата обращения: 10.10.2025).

3. *Милованова, М.М.* Проблемные аспекты изучения и установления личности кибермошенника // Правовое обеспечение суверенитета России: проблемы и перспективы: Сборник докладов XXIV Международной научно-практической конференции и XXIV Международной научно-практической конференции Юридического факультета МГУ им. М.В. Ломоносова в рамках XIII Московской юридической недели. В 4-х частях, Москва, 21–24 ноября 2023 года. — Москва: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. — С. 293-295.

4. *Россинская, Е.Р., Семикаленова, А.И.* Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. — 2020. — № 3. — С. 745-759.

5. *Халиуллин, А.И.* Подходы к определению компьютерной преступности // Проблемный анализ и государственно-управленческое проектирование. — 2011. — Т. 4, № 6. — С. 16-23.

**УШАКОВ Даниил Александрович**

Московский государственный юридический университет имени О.Е. Кутафина (МГЮА),  
обучающийся Института частного права

**s2003413@edu.msal.ru**

125993, Россия, г. Москва, ул. Садовая-Кудринская, 9

НАУЧНЫЙ РУКОВОДИТЕЛЬ:

**БОГАТЫРЕВ Константин Михайлович**

кандидат юридических наук

Московский государственный юридический университет имени О.Е. Кутафина (МГЮА),  
старший преподаватель кафедры криминалистики

**kmbogatyrev@msal.ru**

125993, Россия, г. Москва, ул. Садовая-Кудринская, 9

---

**ПРОБЛЕМЫ УСТАНОВЛЕНИЯ ОБСТОЯТЕЛЬСТВ  
ПРОТИВОПРАВНЫХ ДЕЯНИЙ, СОВЕРШАЕМЫХ В МЕССЕНДЖЕРАХ**

**Аннотация.** Статья посвящена рассмотрению актуальной проблематики раскрытия преступлений, совершаемых с использованием мессенджеров. Проанализирована в динамике статистка преступлений. Изучены и рассмотрены значимые вопросы, связанные прежде всего с технологическими особенностями самих платформ, анонимностью пользователей, правовыми ограничениями и необходимостью сбора цифровых доказательств.

Для решения имеющихся проблем предложены меры по раскрытию преступлений, совершаемых с использованием мессенджеров. Сформулирован вывод о потребности в разработке комплексного подхода, сочетающего правовые, технические и организационные меры в целях эффективности борьбы с исследуемыми преступлениями.

**Ключевые слова:** мошенничество, мессенджеры, киберпреступления, расследование мошенничества, преступность.

D.A. USHAKOV,  
Kutafin Moscow State Law University (MSAL),  
Student of Institute of Private law  
s2003413@edu.msal.ru  
9 Sadovaya-Kudrinskaya Str., Moscow, 125993, Russia

SCIENTIFIC SUPERVISOR:  
K.M. Bogatyrev,  
Candidate of Law,  
Kutafin Moscow State Law University (MSAL),  
Senior lecturer of Criminalistics Department,  
kmbogatyrev@msal.ru  
9 Sadovaya-Kudrinskaya Str., Moscow, 125993, Russia

### **CIRCUMSTANCES OF INSTANT MESSAGING ILLEGAL ACTS: INVESTIGATION PROBLEMS**

**Annotation.** *The article deals with topical issues of solving instant messaging crimes committed. The statistics of crimes were diachrony analyzed. The article provides an analysis of the significant issues such as technological features of the platforms, user anonymity, legal restrictions, and digital evidences.*

*To address the existing issues, measures have been proposed to prevent crimes committed through instant messaging. Therefore, we conclude that it is necessary to develop an integrated approach that combines legal, technical, and organizational measures in order to effectively combat the crimes under investigation.*

**Key words:** *fraud, instant messaging, cybercrimes, fraud investigation, crime.*

Хотя в отечественном научном дискурсе принято говорить об этом явлении как о новом, недавно сформировавшемся, следует принять во внимание, что основной телекоммуникационной сети Интернет, на основе которой функционирует Всемирная паутина, в современном ее виде уже исполнилось 30 лет; о продолжительности его существования свидетельствует хотя бы наличие доменного имени СССР — .su<sup>1</sup>. Да, повсеместное его внедрение в России произошло позже (на рубеже 1990-х — 2000-х; официальной датой возникновения Рунета следует считать 7 апреля 1994 года, когда Россия была зарегистрирована и внесена в международную базу данных с присвоением ей домена RU), и 30 лет в рамках фундаментальных научных исследований не такой большой период, но все же Интернет существует уже достаточно долго, для того

---

<sup>1</sup> Информация о домене SU // Регистратор доменных имен РЕГ.РУ — [Электронный ресурс]. — URL: <https://www.reg.ru/domain/new/SU/info> (дата обращения: 12.10.2025).

чтобы говорить о нем как об изученном явлении<sup>1</sup>. Последовавший за его внедрением рост различных информационных технологий, охарактеризовался не только расширением массовых телекоммуникаций, но и активным их использованием в преступных целях.

Так, в России в сфере Интернет-технологий в 2013 году было зарегистрировано 10 942 преступления, в 2019 году – 120 587 преступлений<sup>2</sup>; в 2024 году это уже 765 400 преступлений (что на 13,1 % больше, чем за период 2023 года)<sup>3</sup>. Удельный вес рассматриваемых противоправных деяний в общем числе преступлений неуклонно растет: доля IT-преступлений в 2020 году – 25%, в 2021 году – 25,8 %, в 2022 году – 26,5 %, в 2023 году – 34,8 %, а в 2024 году – 40 %<sup>4</sup>.

За 6 месяцев 2025 года зарегистрировано 142 191 преступление, совершенное с использованием средств мгновенного обмена сообщениями — интернет-мессенджеров<sup>5</sup>. При этом следует отметить, что только за одну неделю в августе 2025 года с использованием мессенджера Telegram было совершено 414 преступлений, 313 преступлений с помощью WhatsApp (принадлежит Meta, чья деятельность признана в России экстремистской), с использованием социальной сети «ВКонтакте» — 19 преступлений, с использованием социальной сети «Одноклассники» — 1 преступление, с использованием мессенджера Max преступлений не было<sup>6</sup> (хотя позже первый случай дистанционного хищения с использованием мессенджера MAX все же произошел<sup>7</sup>).

---

<sup>1</sup> См.: *Богатырев, К.М.* Разграничение государствами национальных зон ответственности за безопасность в цифровой медиасреде: участие специалиста // Судебная экспертиза. — 2022. — № 3 (71). — С. 18-25.

<sup>2</sup> Портал правовой статистики. — [Электронный ресурс]. — URL: [crimestat.ru](https://crimestat.ru) (дата обращения: 12.10.2025).

<sup>3</sup> Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2024 года. Сайт МВД РФ. — [Электронный ресурс]. — URL: <https://мвд.рф/reports/item/60248328/> (дата обращения: 12.10.2025).

<sup>4</sup> В России в 2024 году IT-преступления достигли пика за последние пять лет // tass.ru. — [Электронный ресурс]. — URL: <https://tass.ru/proisshestviya/22978955/> (дата обращения: 12.10.2025).

<sup>5</sup> МВД России предупреждает: основная часть дистанционных преступлений совершается с использованием мессенджеров. Сайт МВД РФ. — [Электронный ресурс]. — URL: <https://мвд.рф/news/item/68679423/> (дата обращения: 12.10.2025).

<sup>6</sup> См.: Вестник Киберполиции. — [Электронный ресурс]. // Telegram. 03.08.2025. — URL: [https://t.me/cyberpolice\\_rus/](https://t.me/cyberpolice_rus/) (дата обращения: 12.10.2025).

<sup>7</sup> МВД сообщило о первом задержании за мошенничество в MAX // РБК. — [Электронный ресурс]. — URL: <https://www.rbc.ru/society/20/08/2025/68a5a6749a79472e43f4cbea> (дата обращения: 12.10.2025).

В сегодняшнее время раскрытие преступлений, совершаемых с использованием мессенджеров, сталкивается с рядом серьёзных проблем, связанных прежде всего с технологическими особенностями самих платформ, возможностью анонимизации пользователей, правовыми ограничениями и необходимостью сбора цифровых доказательств<sup>1</sup>.

Основной технологической проблемой является сквозное шифрование, поскольку большинство современных мессенджеров, таких, например, как WhatsApp (принадлежит Meta, чья деятельность признана в России экстремистской), ВКонтakte и Telegram, используют данную технологию, делая переписку недоступной для третьих лиц (включая правоохранительные органы). Такое обстоятельство значительно усложняет сбор информации без физического и прямого доступа к устройству. Некоторые мессенджеры предлагают функцию автоматического удаления сообщений (например, секретные чаты в Telegram), что позволяет преступникам принимать меры к уничтожению улик.

Другой проблемой установления противоправных деяний, совершаемых в мессенджерах, является то обстоятельство, что преступники часто маскируют свой IP-адрес, используя виртуальные частные сети VPN или анонимные сети Tor, что затрудняет определение местоположения злоумышленников, их идентификацию и раскрытие преступлений.

Также преступники часто для сокрытия своей преступной деятельности создают анонимные аккаунты, регистрируют их на чужие или вымышленные имена, используют одноразовые SIM-карты. Это делает идентификацию реального пользователя крайне сложной.

Распределенное хранение данных не позволяет оперативно выявлять свершение подобных преступлений, поскольку информация, касающаяся непосредственно преступления, может быть разбросана по разным устройствам и серверам, что затрудняет ее сбор и хранение.

---

<sup>1</sup> *Милованова, М.М.* Криминалистическая превенция телефонного мошенничества / М.М. Милованова // Правовой альманах. — 2025. — № 1(41). — С. 35-36; *Милованова, М.М.* Цифровизация и проблемы расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий / М.М. Милованова // Российская правовая система: в поисках национальной идентичности: Сборник докладов XIV Московской юридической недели. В 6-ти частях, Москва, 26–29 ноября 2024 года. — Москва: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2025. — С. 109.

Установление противоправных деяний, совершаемых в мессенджерах, вызывает правовые и процессуальные сложности, например, необходимость соблюдения судебных процедур, поскольку для получения данных от компаний-разработчиков мессенджеров правоохранным органам необходимо получить постановление суда для проведения оперативных мероприятий, направленных на раскрытие таких преступлений, что является длительным процессом. К тому же, не все компании сотрудничают с властями, особенно если их серверы находятся в других странах. Как известно, разработчик мессенджера Telegram Павел Дуров так и не передал российским правоохранным органам ключи для шифрования сообщений<sup>1</sup>.

При этом следует отметить, что категория рассматриваемых преступлений носит трансграничный характер, так как мессенджеры не имеют географических границ. Если серверы мессенджера расположены в другой стране, расследование может столкнуться с проблемами юрисдикции и межгосударственного сотрудничества. Кроме того, стандарты сбора и представления электронных доказательств могут отличаться в разных странах, что создаёт дополнительную проблему при международном взаимодействии.

Особую проблему вызывает закрепление доказательств, поскольку электронные доказательства легко изменить или уничтожить. Для придания юридической силы переписке в мессенджерах часто требуется нотариальное заверение, что может оказаться невозможным, если преступник уже удалил сообщения.

Еще одной проблемой установления противоправных деяний, совершаемых в мессенджерах, являются методические трудности, заключающиеся в обработке большого объёма информации, поскольку в рамках расследования может быть получено огромное количество данных, включая содержимое чатов, медиафайлы и метаданные, анализ которых требует значительных временных и человеческих ресурсов. При этом данные в мессенджерах можно подделать или отредактировать, что

---

<sup>1</sup> How Telegram's Founder Went From Russia's Mark Zuckerberg to Wanted Man // The New York Times. — [Электронный ресурс]. — URL: <https://www.nytimes.com/2024/08/26/technology/pavel-durov-telegram-founder.html> (дата обращения: 12.10.2025).

ставит под сомнение их достоверность, а взлом аккаунта может позволить преступнику вносить изменения в историю переписки<sup>1</sup>.

В мессенджерах распространены различные виды мошенничества, например, связанные с продажей как разрешенных, так и запрещенных товаров и веществ, подделкой документов или вымогательством, и выявление таких мошеннических схем и установление личностей организаторов требует зачастую специальных навыков<sup>2</sup>.

Недостаток квалификации экспертов и следователей вызывает затруднение в раскрытии указанных преступлений, так как не все сотрудники правоохранительных органов обладают необходимым уровнем подготовки и ресурсами для проведения сложных криминалистических экспертиз цифровых доказательств.

Для решения имеющихся проблем в раскрытии преступлений, совершаемых в мессенджерах, можно рекомендовать несколько мер:

1. Развитие сотрудничества между государственными органами, технологическими компаниями и научными учреждениями для создания платформ обмена информацией, разработки стандартов для расследования и доказывания преступлений в мессенджерах, а также совместного исследования новых угроз и технологий.

2. Внедрение и применение технологий искусственного интеллекта, который можно использовать для автоматического выявления потенциально противоправных сообщений, поведения пользователей и автоматизированного анализа больших объемов данных, что существенно повысит скорость и качество расследований.

3. Обучение и повышение квалификации сотрудников правоохранительных органов в сфере цифровой криминалистики.

4. Информирование и просвещение граждан о способах защиты конфиденциальности и безопасной эксплуатации мессенджеров.

2. Мониторинг эффективности применяемых мер и технологий, своевременное внедрение корректировок и новых решений с учетом динамики развития цифровых технологий и преступных методов.

Таким образом, в заключении можно отметить, что проблемы установления обстоятельств противоправных деяний в мессенджерах

---

<sup>1</sup> См.: *Галяшина, Е.И., Богатырев, К.М., Антонян, Е.А., Кокурин, А.В.* Медиабезопасность в цифровой среде: роль сведущих лиц: Монография. — М.: Проспект, 2024. — 288 с.

<sup>2</sup> См.: *Андрасян, А.В.* Видеокружки Telegram как объект криминалистического исследования при производстве по уголовным делам о мошенничестве // Правовой альманах. — 2025. — № 1 (41). — С. 61-66.

требуют комплексного подхода, сочетающего правовые, технические и организационные меры. Без этого эффективность борьбы с цифровой преступностью будет снижаться, что будет создавать угрозу для общественной безопасности.

#### БИБЛИОГРАФИЯ:

1. *Андрасян, А.В.* Видеокружки Telegram как объект криминалистического исследования при производстве по уголовным делам о мошенничестве // Правовой альманах. — 2025. — № 1 (41). — С. 61-66.
2. *Богатырев, К.М.* Разграничение государствами национальных зон ответственности за безопасность в цифровой медиасреде: участие специалиста // Судебная экспертиза. — 2022. — № 3 (71). — С. 18-25.
3. *Галяшина, Е.И., Богатырев, К.М., Антонян, Е.А., Кокурин, А.В.* Медиабезопасность в цифровой среде: роль сведущих лиц: Монография. — М.: Проспект, 2024. — 288 с.
4. *Милованова, М.М.* Криминалистическая превенция телефонного мошенничества // Правовой альманах. — 2025. — № 1(41). — С. 34-41.
5. *Милованова, М.М.* Цифровизация и проблемы расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Российская правовая система: в поисках национальной идентичности: Сборник докладов XIV Московской юридической недели. В 6-ти частях, Москва, 26–29 ноября 2024 года. — Москва: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2025. — С. 109-112.