Научная статья
УДК 343.9

ИННОВАЦИОННЫЕ ПОДХОДЫ В КРИМИНАЛИСТИКЕ: МЕТОДЫ И ТЕХНОЛОГИИ ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ЗАПРЕЩЕННОЙ ИНФОРМАЦИИ В ЦИФРОВУЮ ЭПОХУ

Руслан Александрович Суханов
Саратовская государственная юридическая академия, г. Саратов, Российская Федерация, rus201993@gmail.com

Аннотация. В статье рассматриваются современные инновационные подходы в криминалистике, направленные на противодействие распространению запрещённой информации в цифровом пространстве. Автор анализирует методы цифровой криминалистики, включая использование искусственного интеллекта, машинного обучения, анализа больших данных и обработки естественного языка для выявления, интерпретации и фиксации цифровых следов. Особое внимание уделяется алгоритмам распознавания экстремистского, порнографического и иного деструктивного контента, а также методам идентификации авторов и соучастников преступной деятельности. Отмечены проблемы анонимности, трансграничности и недостаточной международной координации, а также сложности правового и этического характера. Сделан вывод о необходимости комплексного подхода, сочетающего технические, правовые и организационные меры в рамках цифровой криминалистики.

Ключевые слова: цифровая криминалистика, запрещённая информация, идентификация, экстремизм, анонимность, доказательства, правовое регулирование

Для цитирования: Суханов, Р. А. Инновационные подходы в криминалистике: методы и технологии противодействия распространению запрещенной информации в цифровую эпоху // Криминалистика: вчера, сегодня, завтра. 2025. Т. 34. № 2. С. 184–192.

INNOVATIVE APPROACHES IN CRIMINALISTICS: METHODS AND TECHNOLOGIES FOR COUNTERING THE SPREAD OF PROHIBITED INFORMATION IN THE DIGITAL AGE

Ruslan A. Sukhanov
Saratov State Law Academy, Saratov, Russian Federation, rus201993@gmail.com

Abstract. The article examines modern innovative approaches in Criminalistics aimed at countering the spread of prohibited information in the digital space. The author analyzes Criminalistics methods, including the use of artificial intelligence,

machine learning, big data analysis, and natural language processing for detecting, interpreting, and documenting digital traces. Special attention is given to algorithms for recognizing extremist, pornographic, and other destructive content, as well as techniques for identifying authors and accomplices involved in digital crimes. The study highlights issues related to anonymity, cross-border jurisdiction, and the lack of international coordination, as well as legal and ethical challenges. The article concludes by emphasizing the need for a comprehensive approach that combines technological, legal, and organizational measures within the framework of Criminalistics..

Keywords: Criminalistics, prohibited information, artificial intelligence, identification, extremism, anonymity, evidence, legal regulation

For citation: Sukhanov, R. A. Innovatsionnyye podkhody v kriminalistike: metody i tekhnologii protivodeystviya rasprostraneniyu zapreshchennoy informatsii v tsifrovuyu epokhu [Innovative approaches in criminalistics: methods and technologies for countering the spread of prohibited information in the digital age]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2025, vol. 34 no. 2, pp. 184–192 (in Russ.).

Введение

Распространение запрещённой информации в Интернете – одна из актуальнейших угроз современного цифрового общества. Традиционные методы расследования и анализа оказываются недостаточно эффективными. В условиях цифровой эпохи криминалистика трансформируется, внедряя новые технологии для анализа больших данных, распознавания текста, выявления цифровых следов.

Цель данной работы – исследовать инновационные методы и технологии в цифровой криминалистике, направленные на борьбу с распространением запрещённого контента.

Основная часть

С развитием цифровых технологий человечество получило неограниченный доступ к информации, но наряду с этим возникли риски, связанные с распространением вредоносного и запрещённого контента. Автор согласен с мнением К. И. Рыдченко, что в российском и международном праве под запрещённой информацией понимаются сведения, распространение которых противоречит действующему законодательству, наносит вред обществу, государству или отдельным гражданам [1].

К основным видам запрещённой информации, распространяемой в цифровой среде, относятся:

– экстремистские материалы, включая призывы к насилию, межнациональной или межрелигиозной розни, материалы террористического характера;

– порнография, особенно с участием несовершеннолетних (детская порнография);

– сведения о способах изготовления и распространения наркотических средств и психотропных веществ;

– призывы к самоубийству, информация, провоцирующая членовредительство;

– фейки и дезинформация, распространяемая в целях дестабилизации общественного порядка;

– пропаганда насилия, жестокости, расизма, нацизма, ксенофобии;

– материалы, нарушающие авторские права, распространение нелицензионного ПО, медиафайлов.

Бороться с таким видом информации помогает цифровая криминалистика – это область криминалистической науки и практики, связанная с выявлением, сохранением, анализом и интерпретацией цифровых доказательств. Её развитие обусловлено необходимостью реагировать на преступления, совершаемые с использованием информационных технологий.

Цифровая криминалистика выходит за рамки традиционных методов сбора улик. Сегодня она включает использование искусственного интеллекта, автоматического анализа больших данных, высокоточных инструментов и платформ, способных обрабатывать сложную и многослойную информацию. Однако внедрение инноваций требует высокой квалификации специалистов, правового регулирования и этических гарантий.

Современная цифровая криминалистика развивается на фоне стремительного технологического прогресса, что приводит к радикальным изменениям в подходах к расследованию правонарушений, совершаемых в информационной среде. Если ранее основой цифровой экспертизы был физический осмотр компьютеров и анализ файлов вручную, то в XXI веке в центр внимания всё чаще попадают интеллектуальные системы, способные работать с огромными объёмами цифровых данных и выявлять закономерности, недоступные человеческому восприятию.

Традиционные методы, как правило, включали в себя клонирование жёстких дисков, просмотр файлов, анализ метаданных и восстановление удалённых элементов. Эти действия, хотя и остаются актуальными, больше подходят для изолированных случаев, не связанных с массовым распространением информации. При расследовании преступлений террористической и экстремистской направленности или связанных с оборотом запрещённого контента в Интернете необходимо учитывать скорость, с которой распространяется подобная информация, а также уровень анонимности, предоставляемый цифровыми средствами коммуникации. Эти обстоятельства требуют внедрения более адаптивных и технологичных методов.

Одним из ключевых направлений в развитии цифровой криминалистики стало использование искусственного интеллекта. Он применяется для автоматического анализа контента, определения его принадлежности к категории запрещённого, а также для распознавания поведенческих

шаблонов пользователей [2]. Нейросетевые алгоритмы способны анализировать не только текстовую информацию, но также графические и видеоматериалы, выявляя порнографические изображения, насилие, признаки экстремизма или пропаганду самоубийства. Такие алгоритмы особенно эффективны в тех случаях, когда запрещённый контент маскируется (например, в форме мемов, кодированных сообщений или безобидных на первый взгляд визуальных элементов).

Важную роль играет также машинное обучение, позволяющее программам самообучаться на новых данных и совершенствовать критерии распознавания нарушений. Благодаря этому системы могут своевременно реагировать на изменяющиеся формы деструктивного цифрового контента. В сочетании с методами анализа больших данных это обеспечивает способность обрабатывать миллионы единиц информации в реальном времени и выделять потенциально опасные материалы для последующего изучения специалистами.

Цифровая криминалистика также активно использует технологии обработки естественного языка, позволяющие анализировать тональность, смысловую нагрузку и даже скрытые подтексты в сообщениях пользователей. Системы, основанные на лингвистических алгоритмах, способны выявлять завуалированные призывы к противоправным действиям, которые ускользают от простого фильтра, по ключевым словам. Особенно важно это при мониторинге экстремистских форумов, закрытых чатов и социальных сетей.

Кроме анализа текстов и медиафайлов в цифровой криминалистике растёт значение методик, направленных на отслеживание цифрового следа пользователя. Специалисты могут восстановить цепочку действий злоумышленника, даже если он пытался стереть улики или использовать средства анонимизации. Используются методы обратного анализа, включающие восстановление удалённой информации, анализ истории браузера, логов и сетевой активности, что позволяет идентифицировать не только автора запрещённой информации, но и потенциальных соучастников, распространителей и лиц, вовлечённых в цифровые преступления [3, с. 87]. Это может быть достигнуто через анализ цифровых метаданных, стиль изложения, регулярные ошибки, сохранённые черновики или повторяющиеся шаблоны поведения в сети. При этом следует учитывать возможность подставного контента и использование программ-генераторов, поэтому выводы об авторстве должны базироваться не на единственном признаке, а на совокупности данных, подтверждённых экспертным заключением.

Следователь также обязан учитывать процессуальные аспекты: все действия с цифровыми уликами должны быть оформлены надлежащим образом, с фиксацией цепочки хранения и доступа к информации, соблюдением условий

неизменности файлов, сохранением оригинальных носителей. При необходимости следователь обращается за содействием к специалистам: криминалистам, аналитикам, лингвистам, экспертам в области ИТ.

Эффективность методики напрямую зависит от взаимодействия между следователем, оперативными службами и экспертами. В случае транснационального характера преступления следует активно использовать возможности международной правовой помощи, Интерпола, Европола, а также сотрудничество с транснациональными IT-компаниями и платформами. Особую ценность имеют данные, предоставляемые администраторами доменов, регистраторами и хостинг-провайдерами.

В случае установления личности преступника, занимавшегося оборотом запрещенного контента в цифровом пространстве, ключевой задачей следствия становится комплексное рассмотрение нескольких принципиальных направлений работы. В первую очередь необходимо установить точную роль подозреваемого: был ли он автором запрещённого контента, его распространителем, техническим посредником (например, администратором интернет-ресурса), или действовал в составе организованной группы. От этих обстоятельств зависит правовая квалификация деяния и объём обвинения.

Следующим важным этапом является анализ цифровых следов. Следователю следует инициировать судебную компьютерно-техническую экспертизу и провести исследование всех изъятых электронных устройств: компьютеров, мобильных телефонов, носителей информации, аккаунтов в облачных хранилищах. Особое внимание уделяется восстановлению удалённых файлов, истории интернет-браузера, логам авторизации, метаданным документов и коммуникациям в мессенджерах. Эти данные могут подтвердить факт создания и публикации контента, а также указать на наличие сообщников и обстоятельства совершения преступления.

Следователь обязан также предпринять меры по выявлению и установлению иных лиц, причастных к преступлению. В рамках анализа переписок, списков контактов, социальных сетей и электронной почты важно определить, кто из собеседников мог быть заказчиком, куратором, техническим исполнителем или распространителем запрещённой информации. Выявление координации между участниками, распределения ролей и систематического характера взаимодействия может свидетельствовать о наличии группы лиц по предварительному сговору либо организованного сообщества.

Крайне важно соблюдать процессуальную чистоту. Все действия с цифровыми доказательствами должны быть оформлены

в строгом соответствии с УПК РФ[1]: необходимо фиксировать цепочку хранения электронных носителей, использовать проверенное программное обеспечение при копировании данных, удостоверять хеш-суммы файлов, оформлять протоколы с указанием точного времени, места, технических условий.

Неотъемлемой частью современной цифровой криминалистики стали программные комплексы, автоматизирующие процессы анализа – они позволяют систематизировать и визуализировать данные, выявлять связи между подозреваемыми, анализировать информацию, извлечённую с мобильных устройств и облачных сервисов, а также вести расследование в условиях многозадачности и большого информационного потока.

Распространение запрещённой информации в цифровом пространстве представляет собой одну из наиболее сложных и быстро меняющихся угроз современности. Несмотря на появление эффективных инструментов и методик цифровой криминалистики, на практике существует целый ряд проблем, препятствующих результативному противодействию деструктивному контенту. Эти проблемы носят как технологический, так и организационно-правовой характер и требуют системного подхода к их решению.

Одним из наиболее значимых вызовов остаётся высокая скорость появления и распространения запрещённой информации. В цифровой среде отдельные сообщения могут охватить десятки тысяч пользователей за считаные минуты, особенно если они распространяются через социальные сети, мессенджеры и видеохостинги. Алгоритмы платформ, основанные на вовлечённости, зачастую сами усиливают распространение шокирующего или провокационного контента, не всегда успевая реагировать на его потенциальную незаконность, что создаёт ситуацию, когда механизмы мониторинга и фильтрации оказываются запаздывающими по отношению к динамике цифровых коммуникаций.

Существенное затруднение вызывает также вопрос анонимности пользователей. Использование VPN, сетей Tor, прокси-серверов и других средств анонимизации мешает правоохранительным органам эффективно отслеживать источники противоправной информации. Часто её распространение осуществляется через закрытые сообщества, форумы или анонимные чаты, доступ к которым затруднён не только технически, но и юридически. При этом сами платформы не всегда готовы сотрудничать с национальными следственными органами, ссылаясь на юрисдикционные ограничения, защиту данных пользова-

[1] Российская Федерация. Законы. Уголовно-процессуальный кодекс Российской Федерации : УПК : принят Гос. Думой 22 ноября 2001 года : одобрен Советом Федерации 5 декабря 2001 года : послед. ред. // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 25.04.2025).

телей или корпоративную политику.

Юридическая неопределённость и несогласованность законодательства разных стран также формируют проблему международной координации действий. Распространение запрещённого контента редко ограничивается территорией одного государства. Зачастую серверы, на которых размещается информация, находятся за пределами страны, где она признана незаконной. В таких условиях расследование требует международного правового сотрудничества, которое нередко затруднено различиями в определении самого понятия «запрещённая информация», а также отсутствием унифицированных стандартов регулирования в сфере цифровой безопасности.

С точки зрения правоприменения одной из ключевых проблем остаётся недостаточная квалификация сотрудников правоохранительных органов в области кибербезопасности. Отставание образовательных программ и профессиональной подготовки от практических потребностей приводит к тому, что даже при наличии технических средств не всегда удаётся грамотно собрать и зафиксировать цифровые доказательства, чтобы они имели юридическую силу в суде.

Кроме того, важно учитывать и правозащитные аспекты противодействия распространению запрещённой информации. Излишне агрессивное противодействие противоправной информации может привести к неоправданному ограничению конституционных прав граждан на свободный доступ к информации. Возникают риски чрезмерной цензуры, политической или идеологической мотивации блокировок, что подрывает доверие к институтам цифрового регулирования. Таким образом, важно сохранить баланс между обеспечением информационной безопасности и соблюдением фундаментальных прав человека в цифровом пространстве.

Несмотря на существующие проблемы, цифровая криминалистика обладает огромным потенциалом для дальнейшего развития. В ближайшие годы можно ожидать углубления интеграции искусственного интеллекта в системы анализа цифрового контента, а также появления более совершенных моделей предиктивного мониторинга, позволяющих выявлять угрозы ещё до их массового распространения. Также возрастает значение коллаборации с технологическими компаниями и владельцами интернет-платформ, которые всё чаще разрабатывают собственные системы модерации, основанные на этических кодексах и технических фильтрах. Особое внимание будет уделяться разработке международных соглашений и конвенций, направленных на создание единого цифрового правового поля, позволяющего более эффективно координировать усилия различных государств.

Выводы и заключение

Таким образом, эффективное противодействие распространению запрещённой информации в цифровую эпоху требует не только

совершенствования технических средств, но и глубокого переосмысления принципов регулирования информационного пространства. Только при комплексном подходе, сочетающем технологические, юридические и гуманитарные аспекты, можно выстроить устойчивую и справедливую систему цифровой безопасности.

Скорость цифровой трансформации приводит к снижению эффективности классических подходов к расследованию преступлений в сфере оборота запрещенной информации. Цифровая среда порождает новые формы правонарушений, а высокая скорость обмена данными, анонимность и техническая сложность отслеживания источников информации требуют переосмысления методологических и технических основ криминалистики.

Современные методы, основанные на применении искусственного интеллекта, машинного обучения, анализа больших данных и лингвистических технологий, открывают широкие перспективы для автоматизации и повышения точности выявления противоправного цифрового контента. Программные средства цифровой криминалистики позволяют не только систематизировать и интерпретировать большие массивы информации, но и восстанавливать цепочку действий преступников, а также устанавливать связи между участниками противоправной деятельности.

К числу наиболее острых проблем относятся правовая фрагментарность регулирования, слабая международная координация, ограниченность доступа к зашифрованным каналам связи, а также дефицит квалифицированных специалистов, способных работать на стыке юриспруденции и информационных технологий. Важным остаётся и этический аспект: борьба с деструктивным контентом не должна подрывать фундаментальные свободы граждан, включая право на выражение мнения и получение информации.

Эффективность противодействия распространению запрещённой информации в цифровую эпоху определяется не только уровнем технического оснащения правоохранительных органов, но и готовностью государства выстраивать диалог с технологическими компаниями, формировать гибкую и прозрачную нормативную базу и обеспечивать высококачественную профессиональную подготовку специалистов в сфере цифровой криминалистики.

СПИСОК ИСТОЧНИКОВ

1. *Рыдченко, К. И.* Государственная система защиты несовершеннолетних от воздействия вредоносной информации : монография. М. : Юстицинформ, 2018. 208 с.
2. *Баранов, В. В.* Использование искусственного интеллекта для выявления и предотвращения распространения экстремистской и террористической пропаганды в Интернете //Труды Академии управления МВД России. 2024. № 4 (72). С. 113–128.
3. *Кахрамонов, А.* Инструменты цифровой криминалистики // Наука, инновации и образование: ключевые векторы общественного прогресса. 2024. Т. 1. № 1. С. 84–98.

REFERENCES

1. *Rydchenko, K. I.* Gosudarstvennaya sistema zashchity nesovershennoletnih ot vozdejstviya vredonosnoj informacii : monografiya [State System for Protecting Minors from Harmful Information]. Moscow: Justitsinform, 2023, 215 p. (in Russian).
2. *Baranov, V. V.* Ispol'zovanie iskusstvennogo intellekta dlya vyyavleniya i predotvrashcheniya rasprostraneniya ekstremistskoj i terroristicheskoj propagandy v Internete [Using Artificial Intelligence to Detect and Prevent the Spread of Extremist and Terrorist Propaganda on the Internet]. Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia – Trudy Akademii upravleniya MVD Rossii. 2024, no. 4 (72), pp. 113-128. (in Russian).
3. *Kahramonov, A.* Instrumenty cifrovoj kriminalistiki [Digital Forensics Tools]. Nauka, innovacii i obrazovanie: klyuchevye vektory obshchestvennogo progressa. – Science, Innovation and Education: Key Vectors of Social Progress. 2024, vol. 1, no. 1, pp. 84-98. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Суханов Руслан Александрович, аспирант кафедры криминалистики. Саратовская государственная юридическая академия. 410056, Российская Федерация, г. Саратов, ул. Вольская, 1.

INFORMATION ABOUT THE AUTHOR

Ruslan A. Sukhanov, postgraduate student. Department of Criminalistics. Saratov State Law Academy. 1, st. Volskaya, Saratov, Russian Federation, 410056.