

ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ



**ФОРМИРОВАНИЕ ДОКАЗАТЕЛЬСТВ
В ДОСУДЕБНОМ ПРОИЗВОДСТВЕ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ
СЛЕДОВАТЕЛЕМ ПРОГРАММНЫХ СПОСОБОВ АНАЛИЗА
БОЛЬШИХ ОБЪЕМОВ ДАННЫХ, А ТАКЖЕ ПОИСКА
И АНАЛИТИЧЕСКОЙ ОБРАБОТКИ ИНФОРМАЦИИ
ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ СЕТИ ИНТЕРНЕТ**

Учебное пособие

**Воронеж
2026**

ББК 67.73
УДК 343.985.3
Ф79

Коллектив авторов: Гайдин А. И., Смагин П. Г., Гущин А. Н.,
Савицкая И. Г., Красноруцкая Т. А., Тишкин С. В.

Рецензенты:

*М. М. Буслов – заместитель начальника управления по борьбе с
противоправным использованием информационно-коммуникационных
технологий ГУ МВД России по Воронежской области – начальник отдела,
кандидат юридических наук, полковник полиции;*

*Н. А. Лещева – заместитель начальника контрольно-методического
отдела ГСУ ГУ МВД России по Воронежской области, подполковник юстиции.*

Ф79 **Формирование** доказательств в досудебном производстве на основе
использования следователем программных способов анализа больших
объемов данных, а также поиска и аналитической обработки информации из
открытых источников сети Интернет : учебное пособие / А. И. Гайдин,
П. Г. Смагин, Гущин А. Н., Савицкая И. Г. [и др.]. – Воронеж :
Воронежский институт МВД России, 2026. – 57 с.
ISBN 978-5-00229-303-2

В учебном пособии рассматриваются возможности использования
современных информационных технологий в расследовании преступлений,
способы поиска и анализа информации по открытым ресурсам сети Интернет,
уголовно-процессуальные и тактические особенности фиксации
доказательственной информации, обнаруженной на сетевых ресурсах.

Издание адресовано курсантам и слушателям образовательных
организаций МВД России, преподавателям, студентам юридических вузов и
факультетов, практическим работникам правоохранительных органов.

Ф-40-27(І)-26

ББК 67.73
УДК 343.985.3

ISBN 978-5-00229-303-2

© Воронежский институт МВД России, 2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	4
1. Использование современных информационных технологий в расследовании преступлений.....	6
2. Способы поиска и анализа информации по открытым ресурсам сети Интернет.....	17
3. Уголовно-процессуальные и тактические особенности фиксации доказательственной информации, обнаруженной на ресурсах сети Интернет.....	39
ЗАКЛЮЧЕНИЕ.....	50
БИБЛИОГРАФИЧЕСКИЙ СПИСОК.....	51

ВВЕДЕНИЕ

В последние десятилетия XXI века информационно-телекоммуникационная сеть Интернет получила широкое развитие по всему миру. С каждым годом число пользователей интернетом и компьютерными технологиями неизменно растет. Так, согласно статистике по использованию интернета в 2025 году, более 5,65 миллиардов человек во всем мире пользуются интернетом, что составляет 68,7% населения мира. Основным способ использования интернета – это поиск информации (60,3%)¹.

Информация играет ключевую роль при раскрытии и расследовании преступлений, а интернет на сегодняшний день выступает хранилищем разнообразной информации, которая может быть использована следователем для формирования доказательственной базы по уголовным делам. В связи с этим для эффективного расследования преступлений следователям необходимо уметь использовать возможности современных компьютерных технологий, связанных в том числе с анализом больших объемов данных, полученных в ходе расследования, добыванием информации из открытых источников сети Интернет и формированием на этой основе доказательств в досудебном производстве по уголовным делам.

Формирование компетенций работы с источниками информации в электронном виде, собирания и использования соответствующих доказательств, должно осуществляться на основе учебных материалов, подготовленных по результатам комплексных научных исследований процессуальной формы деятельности, технического и тактического обеспечения производства следственных действий и организационных мероприятий в отношении сетевых источников уголовно-релевантной информации. В представленном учебном пособии нашли свое отражение результаты такого исследования, которые выразились в системе рекомендаций по использованию следователем программных способов анализа больших объемов данных, а также поиска и аналитической обработки информации из открытых источников сети Интернет для формирования доказательств в досудебном производстве.

Также в пособии изложены и иные результаты решения задач исследования: анализа современных достижений в области информационных технологий в контексте возможности их использования при расследовании преступлений; изучения программных методов поиска информации в сети Интернет (OSINT, «Большие данные», «Парсинг»); синтеза программных решений, используемых для поиска и анализа данных в сети Интернет; выявления возможностей программных средств обработки больших объемов данных.

Учебное пособие может использоваться в обучении курсантов и слушателей образовательных организаций МВД России, изучающих дисциплины «Расследование преступлений в сфере компьютерной информации», «Расследование преступлений в сфере экономической деятельности», «Расследование преступлений против личности и собственности».

Материалы учебного пособия могут быть использованы сотрудниками

¹Сколько пользователей интернета в мире? Статистика интернет-медиа. [Электронный ресурс] // URL: <https://inclient.ru/users-internet-stats/> (дата обращения 30.09.2025)

следственных подразделений МВД России в процессе раскрытия и расследования преступлений, а также в формировании доказательственной базы в ходе досудебного производства по уголовным делам и применяться в служебной подготовке сотрудников указанных категорий.

1. ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Всеобщая глобализация и информатизация оказали существенное влияние на современный мир, затронув важнейшие сферы человеческой деятельности. Российская Федерация наряду с мировым сообществом также активно участвует в создании глобального информационного пространства с развитой системой инфокоммуникаций, что подтверждается законодательной политикой нашего государства.

Так, ч. 4 ст. 29 Конституции РФ гарантирует, что «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом»¹. Это положение стало основой для принятия в РФ целого перечня нормативных правовых актов, регламентирующих процесс внедрения информационных технологий во все сферы развития общества, например, Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»². Пункт 2 ст. 2 указанного ФЗ определяет информационные технологии как «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов».

Особенно актуальным является внедрение современных информационных технологий в сферу борьбы с преступностью, которая в последние десятилетия становится все более технологичной и изощренной.

На сегодняшний день эффективное раскрытие многих преступлений требует от сотрудников правоохранительных органов применения технологий, связанных в том числе с анализом больших объемов данных, полученных в ходе расследования, добыванием информации из открытых источников сети Интернет и формированием на этой основе доказательств в досудебном производстве по уголовным делам.

На возможность использования информационных технологий в деятельности сотрудников правоохранительных органов указывают и положения ФЗ «О полиции». Так, в ст. 11 закона определяется, что «полиция в своей деятельности использует достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру», «...беспилотные воздушные, подводные и надводные суда и аппараты, беспилотные транспортные средства и иные автоматизированные беспилотные комплексы, технические средства, средства аудио-, фото- и видеофиксации...», возможности «...информационно-телекоммуникационной сети Интернет, автоматизированных информационных систем, интегрированных банков данных»³.

¹ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). – Российская газета - 4 июля. [Электронный ресурс] // СПС «КонсультантПлюс». / URL: <http://www.consultant.ru> (дата обращения : 26.06.2025).

² Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». / URL: <http://www.consultant.ru> (дата обращения : 26.06.2025).

³ О полиции : Федеральный закон от 07.02.2011 № 3-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». / URL: <http://www.consultant.ru> (дата обращения : 26.06.2025).

В настоящее время использование различных информационных технологий активно используется сотрудниками как оперативных подразделений органов внутренних дел (например, посредством осуществления оперативно-розыскного мероприятия «получение компьютерной информации»¹), так и органами предварительного следствия и дознания при расследовании преступлений, обеспечивая не только оперативный сбор и обработку данных, но и способствуя оптимизации и повышению эффективности их деятельности.

Например, в процессе доказывания по уголовному делу следователь не только использует компьютер и иные средства аудио- или видеофиксации для закрепления результатов следственных или иных процессуальных действий, но и активно применяет различные базы данных, а также специализированное программное обеспечение, направленное на поиск необходимой для расследования уголовного дела информации.

В качестве самых эффективных и широко распространенных программных средств, применяемых органами предварительного расследования в процессе раскрытия и расследования преступлений, можно назвать следующие:

- справочно-правовые информационные системы (СПИС)², которые предоставляют доступ к данным о преступлениях и криминальных связях в различных регионах России. Эти системы позволяют разрабатывать планы расследования, создавать виртуальные модели и получать рекомендации для раскрытия преступлений³;

- информационную систему «Спрут», разработанную МВД России совместно с Институтом проблем информации Российской академии наук, предназначенную для решения важных задач раскрытия и расследования преступлений на разных этапах досудебного производства;

- программный комплекс «Гранд УД», который включает в себя две подсистемы: автоматизированное рабочее место (АРМ) следователя и АРМ руководителя. Комплекс позволяет следователю не только сохранять фабулы и быстро отыскивать в базе нужные уголовные дела, планировать расследование и отслеживать движение по конкретному делу, фиксировать производство следственных действий и составлять процессуальные документы, но и пользоваться справочной информацией по методикам расследования различных видов преступлений;

- дактилоскопическую идентификационную систему «АДИС», созданную для учета следов рук лиц, проходящих по уголовным делам, и работы с большими объемами дактилоскопических карт. Для решения поставленных задач АДИС переходит на первую созданную в нашей стране автоматизированную дактилоскопическую информационную систему «Папилон», которая используется в российских правоохранительных органах с

¹ Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 г. № 144-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». / URL: <http://www.consultant.ru> (дата обращения : 26.06.2025).

² Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (п. 3 ч. 2) [Электронный ресурс] // СПС «КонсультантПлюс». / URL: <http://www.consultant.ru> (дата обращения : 26.06.2025).

³ Салиев А. А. К понятию о роли специальных знаний, используемых в ходе расследования преступлений // European journal of law and political sciences. 2016. № 4. С. 78.

1989 года и основана на методе математического описания папиллярных узоров.

Кроме вышеуказанных наиболее широко применяемых современных информационных технологий можно обозначить еще ряд программных комплексов и систем, применяемых сотрудниками правоохранительных органов при раскрытии и расследовании преступлений, например:

- специализированную территориально распределенную автоматизированную систему Следственного комитета России (СТРАС-СК) с подсистемой гибридного интеллекта «расследование», подсистемами «контроль», «статистика», «банки» по различным категориям уголовных дел;

- автоматизированную систему «Квадрат», разработанную в ИЦ УВД Свердловской области и позволяющую устанавливать связь между возрастом преступника и местом совершения преступления; определять местность, где совершает преступления один и тот же тип преступника; устанавливать места, откуда приезжают и уезжают лица, совершающие преступления¹;

- «фотограмметрические» системы, используемые при производстве осмотра места происшествия, которые помимо обычной фотосъемки обеспечивают построение многомерных пространственных моделей и позволяют воспроизводить динамику событий на основе протоколов осмотра и 3D-фотограмметрии².

Новое поколение фотоаппаратов и видеокамер позволяет изготавливать цветные фотографии в формате 3D, создавать своеобразную виртуальную анимацию, которая может иметь существенное значение для расследования уголовного дела.

Помимо информационных технологий, представленных в виде различных программных продуктов, справочных и информационных систем, в процессе раскрытия и расследования преступлений сотрудники правоохранительных органов активно используют глобальную сеть Интернет, которая позволяет оперативно получать необходимую и актуальную для расследования уголовного дела информацию, а также общаться с гражданами в режиме реального времени (онлайн).

По мнению Е. П. Ищенко, «основная цель использования интернета в расследовании преступлений – поиск и передача из сети необходимой криминалистически значимой информации в целях ее последующей аналитической обработки³».

Одним из средств поиска информации по интернет-источникам для нужд уголовного судопроизводства являются инструменты OSINT (open source intelligence)⁴, представляющие собой разведку на основе открытых источников⁵

¹ Ваценко А. А. Обзор техник компьютерной криминалистики // Бюллетень науки и практики. 2020. № 6. С. 164-170.

² Терехов А. М. Моделирования и прогнозирования преступности: теоретический аспект // Юридическая наука и практика : Вестник Нижегородской академии МВД России. 2021. № 2. С. 125.

³ Ищенко Е. П., Топорков А. А. Криминалистика : учебник / под ред. Е. П. Ищенко. 2-е изд., испр., доп. и перераб. Москва : КОНТРАКТ, ИНФРА-М, 2010. - С.416.

⁴ Зазулин А. И. Osint для адвоката. Как работать и источниками информации в интернете // Уголовный процесс. 2021. № 10(202). – С. 95.

⁵ ГОСТ Р 59926-2021/ISO/IEC TR 20547 2:2018. «Национальный стандарт Российской Федерации. Информационные технологии. Эталонная архитектура больших данных. Часть 2.

без нарушения законодательства, что отличает OSINT от других форм разведки. Несмотря на то, что изначально OSINT был создан в США для обработки и анализа разведывательных данных, на сегодняшний день он может применяться в российском уголовном процессе при работе с большими объемами данных в рамках доказывания по уголовным делам¹.

В настоящее время OSINT как инструмент собирания электронной информации находит законодательное закрепление в приказе Минцифры России от 7 апреля 2020 г. № 162. Сведения о программном комплексе «Виток-OSINT» включены в реестр российского программного обеспечения как «система сбора, хранения, обработки, анализа, моделирования и визуализации массивов данных»².

Использование технологии OSINT в ходе производства по уголовному делу осуществляется с помощью открытых, находящихся в общем доступе интернет-ресурсов, что исключает необходимость получать санкцию суда на производство следственного действия.

Так, А. Б. Смушкин полагает применять инструменты OSINT с целью исследования открытых интернет-ресурсов или мессенджера «Телеграм» для установления факта первичного поиска клиентов для криминального бизнеса³.

По мнению К. Ю. Яковлевой, следственным действием, уголовно-процессуальная форма которого позволяет применить технологию OSINT, является обыск, осуществляемый в местах нахождения электронной информации⁴.

Целью такого обыска является поиск на интернет-ресурсах электронной информации, которая может стать доказательством по уголовному делу; местом производства – адреса конкретных сайтов, места расположения серверов независимо от их размещения в юрисдикции конкретного государства. Для фиксации производства обыска в местах нахождения электронной информации К. Ю. Яковлева предлагает привлекать не менее двух понятых или применять технические средства фиксации, о чем следует дополнительно указать в ст. ст. 170 и 182 УПК. В качестве примеров использования технологии OSINT при

Варианты использования и производные требования» (утв. и введен в действие Приказом Росстандарта от 2 декабря 2021 г. № 1685-ст). Москва : ФГБУ «РСТ», 2022. URL: <https://clck.ru/35xtY4> (дата обращения : 26.06.2025).

¹ Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет // Алтайский юридический вестник. 2022. № 2 (38). С. 133.

² О включении сведений о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных (Приложение № 1) : приказ Минкомсвязи России от 07.04.2020 № 162. URL: <https://clck.ru/35xsDo> (дата обращения : 26.06.2025). Реестр программного обеспечения. URL: <https://reestr.digital.gov.ru/reestr/307657> (дата обращения : 26.06.2025).

³ Смушкин А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. № 3. С. 103.

⁴ Яковлева К. Ю. Использование технологии OSINT в ходе обыска места нахождения электронной информации // Проблемы правовой и технической защиты информации. 2023. №11. С. 131-136.

производстве обыска автор ссылается на протоколы мониторинга и осмотра интернет-сети, а также осмотра публикаций в мессенджере «Телеграмм»¹.

Резюмируя вышеизложенное, следует отметить, что применение инструментов OSINT при поиске и анализе электронной информации из открытых интернет-источников может расширить возможности производства следственных действий, что приведет к повышению эффективности расследования преступлений.

Говоря о внедрении современных информационных технологий в деятельность правоохранительных органов, следует обратить внимание на такое перспективное сегодня направление для раскрытия и расследования преступлений, набирающее популярность, как технологии «искусственного интеллекта».

В Российской Федерации основным нормативным правовым актом в сфере развития технологии искусственного интеллекта на сегодняшний день является Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года». Стратегия определяет понятия «искусственный интеллект», «технологии искусственного интеллекта», формулирует цели и основные задачи развития искусственного интеллекта в РФ, а также меры, направленные на его использование в целях обеспечения национальных интересов, в том числе в области научно-технологического развития².

Очевидно, что в настоящее время при раскрытии и расследовании преступлений сотрудники правоохранительных органов все больше сталкиваются с необходимостью анализировать большие объемы информации, выявлять скрытые связи и паттерны, а также прогнозировать возможные сценарии развития дела. Представляется, что в таких случаях использование искусственного интеллекта может оказать неоценимую помощь в расследовании уголовного дела и стать эффективным инструментом для улучшения результатов расследования.

Примером использования искусственного интеллекта при расследовании преступлений можно назвать применение GPT (Generative Pre-trained Transformer) – архитектуры нейросети, придуманной разработчиками «Google» и обучаемой на основе больших объемов текстовых данных.

Применительно к производству по уголовному делу эта модель искусственного интеллекта способна анализировать большие объемы данных, выявлять скрытые связи и прогнозировать развитие событий. Например, нейросети на основе архитектуры GPT могут генерировать гипотезы, составлять планы расследования и анализировать материалы уголовных дел.

Так, Р. С. Хамидуллин в рамках эксперимента, проводимого во взаимодействии с Главным следственным управлением по Свердловской

¹ Яковлева К.Ю. Использование технологии OSINT в ходе обыска места нахождения электронной информации // Проблемы правовой и технической защиты информации. 2023. №11. С. 131-136.

² О развитии искусственного интеллекта в Российской Федерации: указ Президента РФ от 10 октября 2019 г. № 490, которым была утверждена Национальная Стратегия развития искусственного интеллекта на период до 2030 г. [Электронный ресурс] // СПС «КонсультантПлюс». URL: <http://www.consultant.ru> (дата обращения : 26.06.2025).

области, в своей работе¹ демонстрирует возможности искусственного интеллекта, используемого при расследовании преступлений по материалам реальных уголовных дел, находящихся в производстве следователей.

Результаты проведенного автором эксперимента показывают, что искусственный интеллект, на примере чата GPT, в процессе расследования преступления может детально и объективно анализировать необходимые в рамках расследования мероприятия, оказывать помощь при постановке вопросов эксперту, определять обстоятельства и места совершения преступлений, а также предотвращать их совершение.

При правильном применении искусственный интеллект может существенно ускорить процесс анализа необходимой информации, планирования расследования, выдвижения следственных версий на всех этапах расследования, став ценным инструментом в руках следователя и повысив эффективность работы правоохранительных органов в целом.

Очевидно, что возможности искусственного интеллекта при расследовании преступлений и для противодействия преступности еще не до конца изучены и представляются крайне перспективными.

При этом, с одной стороны, в отличие от мышления человека искусственный интеллект может быстро обработать и проанализировать гигантские объемы нужной информации, учитывая при этом только объективные обстоятельства и факты, и не имеет склонности к субъективным оценкам, что обеспечивает достоверность сделанных им выводов и результатов.

С другой стороны, на недостоверность или ошибочность выводов искусственного интеллекта могут повлиять как отсутствие человеческой интуиции, эмоционального опыта, так и неполные или некорректные входные данные.

Таким образом, несмотря на очевидную помощь сотрудникам правоохранительных органов при раскрытии и расследовании преступлений, искусственный интеллект все же не может полностью заменить человека, хотя и является крайне перспективным направлением для успешного развития уголовного судопроизводства.

Представляется, что для успешной интеграции искусственного интеллекта в деятельность правоохранительных органов необходимо уделять внимание обучению нейросетей криминалистическим методам и средствам расследования преступлений.

Развитие современных информационных технологий и использование их результатов в уголовном судопроизводстве формирует новые направления для перспективных исследований в этой сфере.

Так, в научной литературе и периодических изданиях учеными все больше акцентируется внимание на внедрении в уголовный процесс электронного уголовного дела, перехода с бумажного на электронный документооборот, использование математических алгоритмов при принятии процессуальных решений, внедрение робототехники и т. д.², а в УПК РФ,

¹ Хамидуллин Р. С. Криминалистическое обеспечение использования технологии искусственного интеллекта в раскрытии и расследовании преступлений // Электронное приложение к «Российскому юридическому журналу». 2024. № 2. С. 19–29. DOI: 10.34076/22196838_2024_2_19.

² Зуев С. В. О современной концепции развития информационных технологий в уголовном судопроизводстве (РИТВУС) // Пермский юридический альманах. 2019. № 2. С. 620.

например, нашло закрепление использование информационных технологий в части изъятия электронных носителей информации и копирования с них информации при производстве следственных действий (ст. 164.1 УПК РФ).

При этом, несмотря на очевидное влияние информационных технологий на уголовное судопроизводство, в настоящее время среди ученых отсутствует единое представление о понятии и сущности электронного доказательства, его места в системе доказательств, особенностях собирания, фиксации оценки и допустимости такого вида доказательств. Различные авторы по-разному формулируют как само определение электронных доказательств, так и их сущность.

Так, по мнению Л. Б. Красновой¹, В. Б. Вехова², электронные доказательства – это вещественные доказательства. А. В. Ткачев указывает, что электронное доказательство относится к категории иных документов³. П. С. Пастухов и В. В. Терехин полагают, что электронное доказательство может иметь три разновидности: иной документ, вещественное доказательство и заключение компьютерно-криминалистической экспертизы⁴.

Исчерпывающего перечня электронных доказательств на сегодняшний день также не существует.

По мнению В. Б. Вехова, Б. П. Смагоринского, С. А. Ковалева, к электронным доказательствам следует относить базы данных, информационные системы, программы для ЭВМ, файлы, сетевые адреса, доменные имена, электронные документы, сообщения, подписи, журналы, денежные средства, сайты и страницы сайтов в сети Интернет⁵.

А. Ю. Черданцев включает в вышеуказанный перечень: записи транзакций; основные деловые записи; почтовый трафик; записи, хранящиеся у третьих лиц (например, провайдер облачных данных); журналы контроля доступа; конфигурации, события, ошибки и другие внутренние файлы; журналы интернет-активности; антивирусные «логи»; журналы обнаружения вторжений; резервные носители; телефонные журналы; телефонные записи; записи «закрытой системы видеонаблюдения»⁶.

Таким образом, несмотря на отсутствие единого мнения в научной литературе по поводу понятия, сущности и видов электронных доказательств, большинство авторов все же относят электронное доказательство к новому

¹ Краснова Л. Б. Электронные носители информации как вещественные доказательства // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4-2. С. 257).

² Вехов В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. 2013. № 10. С. 22–24.

³ Ткачев А. В. Вопросы использования электронных носителей компьютерной информации в уголовном процессе в качестве доказательств иных документов // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 440.

⁴ Пастухов П. С., Терехин В. В. К вопросу о понятии и сущности электронных доказательств в уголовном процессе // Вестник Коми Республиканской академии государственной службы и управления. Серия: Государство и право. 2014. № 18. С. 73.

⁵ Вехов В. Б., Смагоринский Б.П., Ковалев С.А. Электронные следы в системе криминалистики // Судебная экспертиза. 2016. № 2 (46). С. 10–19.

⁶ Черданцев А. Ю. Понятие цифровых доказательств, современное состояние и их роль в доказательственном процессе // Юридическая наука и практика. 2019. Т. 15, № 4. С. 57.

виду доказательств¹, представляющих собой сведения, хранящиеся или передаваемые в цифровой форме, которые надлежащие субъекты могут использовать для установления обстоятельств, входящих в предмет доказывания или иных обстоятельств, имеющих значение для уголовного дела.

Уникальность электронных доказательств заключается в форме представления, способах создания и обработки, а также в высокой степени объективности. Несмотря на отсутствие единого определения в законодательстве, их роль в современном судопроизводстве продолжает расти.

Порядок собирания, изъятия, фиксации и оценки допустимости электронных доказательств

В практике правоохранительных органов все чаще возникает потребность в использовании электронных доказательств при раскрытии и расследовании преступлений. В правоприменительной деятельности стало обычным явлением предоставление в качестве доказательств скриншотов переписок с мобильных устройств, распечаток сообщений из социальных сетей, удалённых аудиофайлов, сохранённых в памяти смартфонов, а также переписок в мессенджерах, таких как WhatsApp или Telegram.

Причем цифровые данные представляются в качестве доказательств в суде не только стороной обвинения, но и стороной защиты, несмотря на то что могут быть легко изменены или уничтожены даже в ходе осмотра, а критерии их допустимости в УПК РФ до настоящего времени отсутствуют, существенно затрудняя их использование в доказывании.

Порядок собирания электронных доказательств имеет свою специфику, которая отличается от собирания традиционных видов доказательств. Разница выражается не только в необходимости «участия специалиста при изъятии определенных видов носителей электронной информации»², но и в том, что в ходе следственного действия изымается не конкретный файл, а электронное устройство, содержащее информацию, имеющую значение для расследования конкретного уголовного дела. Таким образом, можно выделить следующие особенности собирания электронных доказательств³:

- соблюдение общих принципов сбора доказательств;
- привлечение специалиста с соответствующим оборудованием и программным обеспечением;
- недопустимость любых действий, способных изменить цифровые доказательства как до, так и во время их собирания;
- необходимость документирования всех действий, связанных с обращением с цифровыми доказательствами, чтобы обеспечить возможность их проверки заинтересованными лицами – участниками уголовного процесса;
- ответственность должностного лица за все операции с электронными доказательствами;
- обеспечение надлежащей транспортировки и хранения цифровых доказательств с учетом их категории и содержащейся информации.

¹ Зигура Н. А. Компьютерная информация как вид доказательств в уголовном процессе России : дис. ... канд. юрид. наук. Челябинск, 2010. 234 с.

² Осипенко А. Л., Гайдин А. И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник Воронежского института МВД России. 2014. № 1. С. 156-163.

³ Желева О. В. К вопросу о понятии электронных доказательств и критериях допустимости их использования // Уголовная юстиция. 2021. № 17. С. 44-48.

На сегодняшний день в действующем УПК РФ содержатся лишь фрагментарные нормы, регулирующие изъятие компьютерных данных (ст. 164.1) и только по делам экономической направленности.

Исходя из этого, применение электронных средств в доказывании сопряжено как с отсутствием их четкой правовой регламентации, так и с рядом проблем, связанных с изменчивостью цифровых данных. К ним можно отнести:

- специфику хранения информации (так, значительный объем данных находится у специализированных субъектов (провайдеров, хостинг-компаний, отсюда технические сложности при получении и фиксации таких сведений);

- уязвимость цифровых носителей (электронная информация подвержена рискам несанкционированного изменения или полного уничтожения, технологическое устаревание оборудования создает угрозу потери данных);

- проблемы верификации (затруднена идентификация первоисточника цифровых файлов, сложности с установлением подлинности многократно копируемых данных).

Безусловно, все это влияет на достоверность и, соответственно, на допустимость цифровых доказательств. При этом можно согласиться с О. В. Желевой, которая указывает, что сохранность цифровых данных в неизменном виде отражает только технические критерии их допустимости в качестве доказательств и не учитывает правовые (юридические) критерии, которые до сих пор не выработаны ни наукой, ни правоприменительной практикой¹.

Следует отметить, что критерии, применяемые к традиционным видам доказательств (например, получение уполномоченным субъектом, надёжность источника, установленная законом форма закрепления), не всегда подходят для цифровых данных и не решают проблему их допустимости². Кроме того, ни одно из закреплённых в УПК РФ следственных действий не отражает особенности обнаружения и изъятия цифровых данных, на что неоднократно обращали внимание отечественные ученые, указывая на необходимость закрепления в законе новых следственных или процессуальных действий, таких как, например, копирование информации³, обыск компьютерного устройства⁴.

Очевидно, что электронные доказательства, как и любые другие, должны соответствовать критериям достоверности (подтверждать реальные факты), допустимости (иметь форму, отвечающую требованиям закона), относимости (должна существовать логическая связь между доказательствами, сведениями и обстоятельствами преступления).

Отечественные процессуалисты отмечают, что электронные

¹ Желева О. В. К вопросу о понятии электронных доказательств и критериях допустимости их использования // Уголовная юстиция. 2021. № 17. С. 44-48.

² Лазарева В. А. Доказывание в уголовном процессе. Москва, 2009. С. 163-169.

³ Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис... канд. юрид. наук. Москва, 2020. С 14; Григорьев О. Г. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства : автореф. дис....канд. юрид. наук. Омск, 2003. С. 21-22; Овсянников Д. В. Копирование электронной информации как средство уголовно-процессуального доказывания : автореф дис. ... канд. юрид. наук. Екатеринбург, 2015. С. 14-15).

⁴ Зуев С. В., Титова А. С. Слабые стороны информационного подхода в свете цифровизации уголовного судопроизводства // Правопорядок: история, теория, практика. 2019. № 1. С. 52.

доказательства должны:

- быть идентифицированы (определен источник происхождения);
- аутентифицированы (установлена подлинность данных);
- верифицированы (по дате, времени и способу создания и изменения);
- сохранять целостность (должны отсутствовать изменения);
- быть воспроизводимыми (возможность демонстрации)¹.

Таким образом, для электронных доказательств необходимы дополнительные критерии допустимости, не имеющие значения для «традиционных» видов доказательств, в частности – обеспечение их сохранности в неизменном виде с момента получения.

В связи с этим К. А. Титова, И. В. Литвинова предлагают проводить проверку и оценку цифровых данных в три этапа, объединяющих в себе как юридические, так и технические требования к допустимости доказательств. По итогам такой оценки субъектом доказывания должно приниматься решение об их допустимости или недопустимости. Эти этапы включают в себя:

- проверку законности изъятия цифровых данных;
- оценку целостности доказательств через анализ процедуры цифровой экспертизы, используемого оборудования и квалификации экспертов;
- оценку подлинности, целостности и достоверности цифровых данных на основе процедуры экспертизы. Доказательство признается допустимым, если оно помогает установить обстоятельства преступления, сохраняет неизменность на протяжении экспертизы, а результаты признаны достоверными и соответствующими требованиям².

Что касается еще одного критерия допустимости доказательств – установленной законом формы их фиксации, то его применение к электронным доказательствам также вызывает сложности ввиду того, что их нельзя отнести ни к вещественным доказательствам, ни к иным документам, что ставит вопрос об их закреплении в УПК РФ в качестве нового вида доказательств.

Отсутствие в действующем уголовно-процессуальном законе критериев допустимости электронных доказательств формирует специфику их признания в качестве доказательств судами.

В одних случаях они признаются допустимыми только если их содержание подтверждается другими, «неэлектронными» доказательствами³, в

¹ Зуев С. В. О современной концепции развития информационных технологий в уголовном судопроизводстве (РИТВУС) // Пермский юридический альманах. 2019. № 2. С. 620.

² Титова К. А., Литвинова И. В. К вопросу о возможности применения существующих критериев допустимости доказательств к электронным доказательствам в Российском уголовном процессе // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2022. № 2(91). С. 144-151.

³ Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Рос. Федерации от 13 декабря 2018 г. по делу № 4-АПУ18-41 [Электронный ресурс] // Legalacts.ru: законы, кодексы и нормативными правовые акты в Рос. Федерации. URL: <https://legalacts.ru/sud/apellia-tsionnoe-opredelenie-ver-khovnogo-suda-rf-ot-13122018-n-4-arul8-41/> (дата обращения: 09.06.2025); Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Рос. Федерации от 10 декабря 2019 г. по делу № 223-АПУ19-1 [Электронный ресурс] // Судебные и нормативные акты Рос. Федерации. URL: <https://sudact.ru/vsrf/-doc/pQ6xljelyiVL/> (дата обращения: 26.06.2025); Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Рос. Федерации от 3 июля 2013 г. по делу № 46- АПУ13-10 // Сайт Верховного Суда Рос. Федерации. URL:

других случаях электронные доказательства признаются допустимыми даже несмотря на нарушения, допущенные при их получении¹.

Подытоживая вышеизложенное, следует отметить, что в целях дальнейшего эффективного использования электронных доказательств в российском уголовном процессе следует закрепить в УПК РФ не только их понятие, но и порядок собирания, фиксации, оценки электронных доказательств; разработать и закрепить критерии их допустимости, а также регламентировать процессуальные права и обязанности лиц, привлекаемых для работы с электронными доказательствами при одновременном сохранении конституционных гарантий заинтересованных участников уголовного судопроизводства.

Контрольные вопросы

1. Сформулируйте понятие информационных технологий.
2. Какие виды современных информационных технологий активно применяются в деятельности полиции и иных правоохранительных органов?
3. Сформулируйте понятие OSINT.
4. Назовите средства OSINT и возможные направления использования метода в правоохранительной деятельности.
5. Сформулируйте понятие искусственного интеллекта.
6. Перечислите особенности собирания доказательств в электронно-цифровой форме (электронных доказательств).
7. Назовите известные Вам критерии допустимости цифровых доказательств.

<https://vsrf.ru/lk/practice/cases/5567789#55677-89> (дата обращения: 26.06.2025).

¹ Приговор Комсомольского районного суда г. Тольятти от 10 февраля 2020 г. по делу № 1-9/2020 (1- 408/2019) [Электронный ресурс] // Сайт Комсомольского районного суда г. Тольятти. URL: https://kom-somolsky-sam.sudrf.m/modules.php?name=sud_delo&name_op=case&_id=162685477&_uid=6e33ecdb-4355-4475-8ac5-3c57de787e5-d&_deloId=1540006&_caseType=0&_new=0&srv_num=1 (дата обращения: 26.06.2025); Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Рос. Федерации от 26 декабря 2012 г. по делу № 48-012-112 [Электронный ресурс] // Сайт Верховного Суда Рос. Федерации. URL: <https://vsrf.ru/lk/practice/cases/5575441#5575441> (дата обращения: 26.06.2025); Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Рос. Федерации от 5 июня 2020 г. по делу № 225-АПУ20-3 [Электронный ресурс] // Legalacts.ru: законы, кодексы и нормативными правовые акты в Рос. Федерации. URL: <https://legalacts.rii/sud/apelliatsionnoe-opredelenie-sudebnoi-kollegii-po-delam-voennosluzhashchikh-verkhovnogo-suda-rossiiskoi-federatsii-ot-05062020-n-225-ari20-3/> (дата обращения: 26.06.2025); Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Рос. Федерации от 1 августа 2019 г. по делу № 67-АПУ19-8 [Электронный ресурс] // Legalacts.ru: законы, кодексы и нормативно-правовые акты в Рос. Федерации. URL: <https://legalacts.ru/sud/apelliatsionnoe-opredelenie-sudebnoi-kollegii-po-ugolovnym-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-01082019-n-67-apul98/> (дата обращения: 26.06.2025); Конвенция о защите прав человека и основных свобод (ратифицирована 4 ноября 1950 г. в г. Риме) [Электронный ресурс] // Сайт Совета Европы. URL: <https://www.coe.int/ru/web/compass/the-european-convention-on-human-rights-and-its-proto-cols> (дата обращения: 26.06.2025).

2. СПОСОБЫ ПОИСКА И АНАЛИЗА ИНФОРМАЦИИ ПО ОТКРЫТЫМ РЕСУРСАМ СЕТИ ИНТЕРНЕТ

Среди основных способов поиска криминалистически значимой и ориентирующей информации в сети Интернет можно выделить 3 направления:

1. Разведка (поиск информации) по открытым источникам общедоступной сети Интернет («OSINT»), которая предполагает использование ресурсов в рамках правового поля: поисковые сервисы, изучение и анализ текстовых файлов, изображений, видеофайлов, размещенных в открытом доступе самими пользователями.

2. Использование ресурсов закрытой части интернета («Тор», «P2P», «I2P»), которые используются с целью анонимизации пользователей для обмена файлами, работы с мессенджерами и создания анонимных веб-сайтов и сервисов.

3. Использование сервисов и ботов (к примеру, «Глаз Бога», «Himera-search»), осуществляющих поиск информации по базам данных с конфиденциальной информацией, попавшей в сеть путем незаконного копирования.

В рамках настоящего исследования мы проведем анализ способов поиска информации только в открытых источниках сети Интернет.

Язык запросов «Яндекс»

Поисковые системы Яндекс и Google используют сложные алгоритмы для анализа поисковых обращений. Оба сервиса учитывают морфологию слов и их части речи. По умолчанию часть речи сохраняется, а морфология не учитывается.

Например, следователю необходимо найти в информации в сети Интернет о продаже похищенного товара. При запросе «Куплю самовар из серебра 18 века» поисковые системы будут искать страницы, содержащие слова «купить», «самовар», «серебро» в различных формах. Это может привести к показу результатов, не соответствующих точному намерению следователя (к примеру, объявления о покупке самоваров вместо объявлений об их продаже). Для уточнения контекста запроса и получения более релевантных результатов необходимо использовать специальные операторы, предоставляемые поисковыми системами.

Обе системы позволяют использовать операторы, учитывать морфологию, регистр и метасимволы для построения сложных обращений к сети.

Яндекс предоставляет обширную справочную систему по языку обращений. Система позволяет уточнять запросы различными способами.

1. Фиксация морфологической формы слова. Оператор «!» в языке запросов Яндекса используется для фиксации морфологической формы слова. Например, запрос «!Куплю самовар» найдет только страницы, содержащие точную форму «куплю», исключая другие формы глагола «купить».

2. Присутствие указанного слова. Оператор «+» в Яндексе указывает на обязательное присутствие следующего за ним слова в результатах поиска.

3. Поиск по цитате. Для поиска точного вхождения фразы в Яндексе используются кавычки. На запрос «Медицинская книжка без комиссии» сеть покажет страницы, содержащие именно эту фразу в указанном порядке.

4. Цитата с пропущенным словом. Символ «*» в запросах Яндекса обозначает пропущенное слово. Запрос «Сделать * паспорт» найдет фразы типа «сделать российский паспорт» или «сделать заграничный паспорт».

5. Оператор логическое И. Оператор «&&» в Яндексе используется для поиска страниц, содержащих слова в пределах одного документа.

6. Минус-слово. Оператор «-» в Яндексе исключает из результатов поиска страницы, содержащие указанное слово.

7. По заданному адресу. Оператор «url:» в Яндексе позволяет искать информацию по конкретному URL-адресу. Например, «url:https://avito.ru» найдет все страницы на указанном домене.

8. По указанному сайту. Оператор «site:» в Яндексе используется для поиска информации на конкретном сайте, включая все его домены и поддомены.

9. В файлах определенного типа. Оператор «mime:» в Яндексе позволяет искать файлы определенного типа, например «mime:png» найдет изображения с расширением .png.

10. По дате последнего изменения сайта. Оператор «date:» в Яндексе позволяет искать ресурсы по дате в формате: YYYYMMDD. Символ «*» может обозначать любое значение месяца или дня. Например, «date:2025*» найдет страницы, обновленные в 2025 году.

Более подробно ознакомиться с документацией Яндекса можно по адресу: <https://yandex.ru/support/search/ru/query-language/search-context>, Google: https://www.google.com/advanced_search.

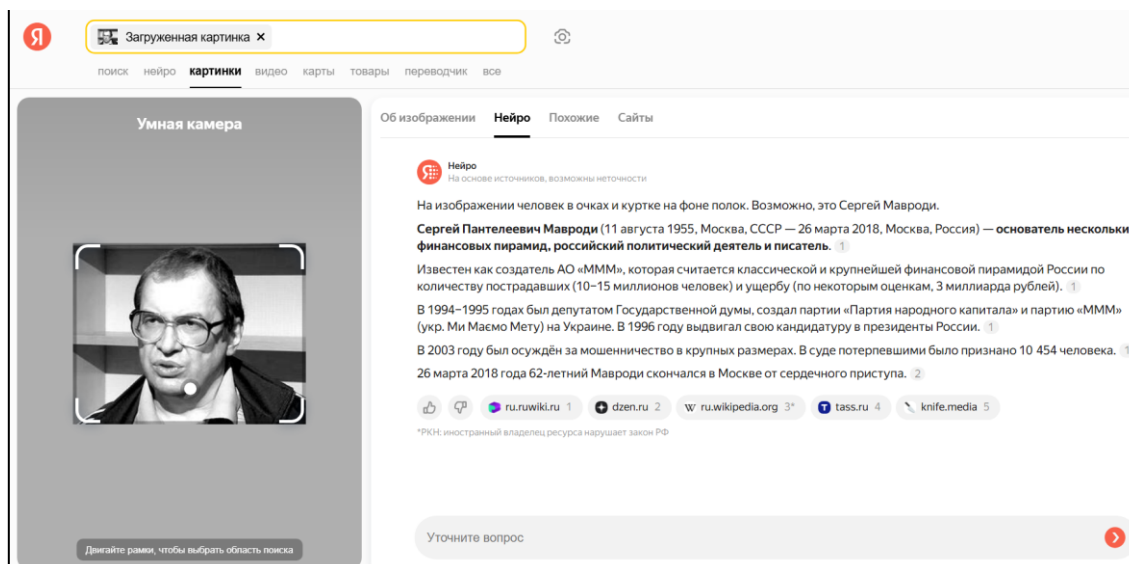
Поиск по фотографии

Поиск в Яндексе по изображению доступен по адресу: <https://yandex.ru/images>. С помощью этого сервиса можно найти источник изображения – определить, где оно было опубликовано впервые, найти похожие изображения – система предложит похожие картинки, определить объект на фото – например, породу собаки, название растения или бренд одежды, проверить оригинальность фото – определить, является ли изображение уникальным или его использовали на других сайтах, найти товары в интернет-магазинах – если на изображении есть предмет (например, кроссовки или смартфон), поиск может найти аналогичные товары с ценами и ссылками на магазины. Для использования достаточно загрузить картинку с устройства или вставить ссылку, после чего сервис покажет результаты с совпадающими и похожими изображениями.

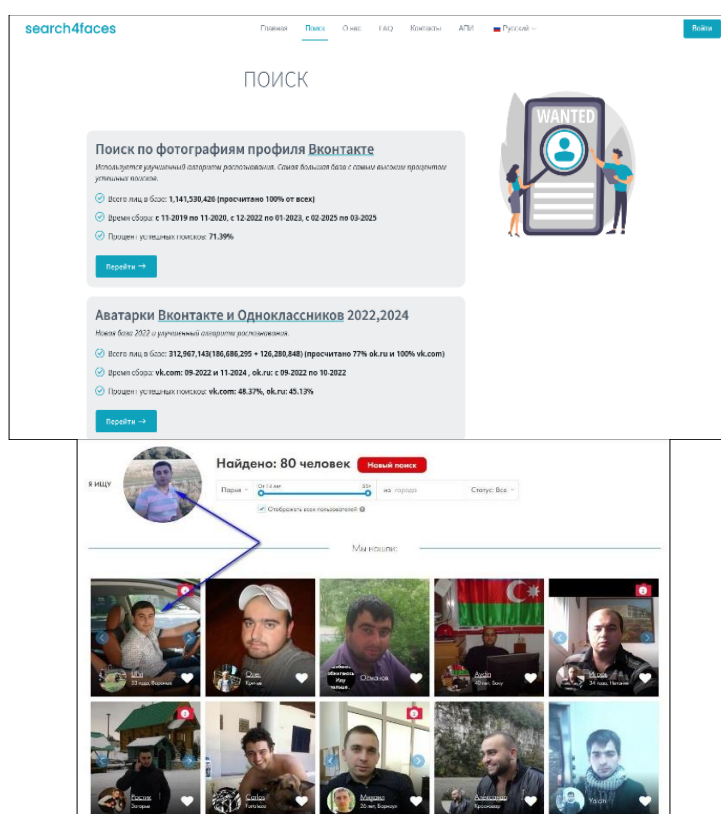
Для идентификации по фотографии лиц, представляющих интерес для процесса расследования по уголовному делу, можно воспользоваться несколькими способами.

Если имеется фотография лица, то можно найти аналогичную фотографию в сети Интернет. Для поиска можно воспользоваться возможностями сайтов «Яндекс» и «Google», которые в разделе «Картинки» позволяют осуществить поиск по сети аналогичной фотографии.

1. Поиск в Яндексе по изображению доступен по адресу: <https://yandex.ru/images>. Формат ответа поисковой сети предполагает описание изображения с использованием нейросети, поиск похожих фотографий в сети Интернет, а также перечень сайтов, где имеется похожее изображение.



2. Сервисы, позволяющие производить поиск по социальным сетям. К примеру, на сайте <https://search4faces.com/search.html> доступен поиск по профилям и аватарам социальных сетей «ВКонтакте», «Одноклассники».



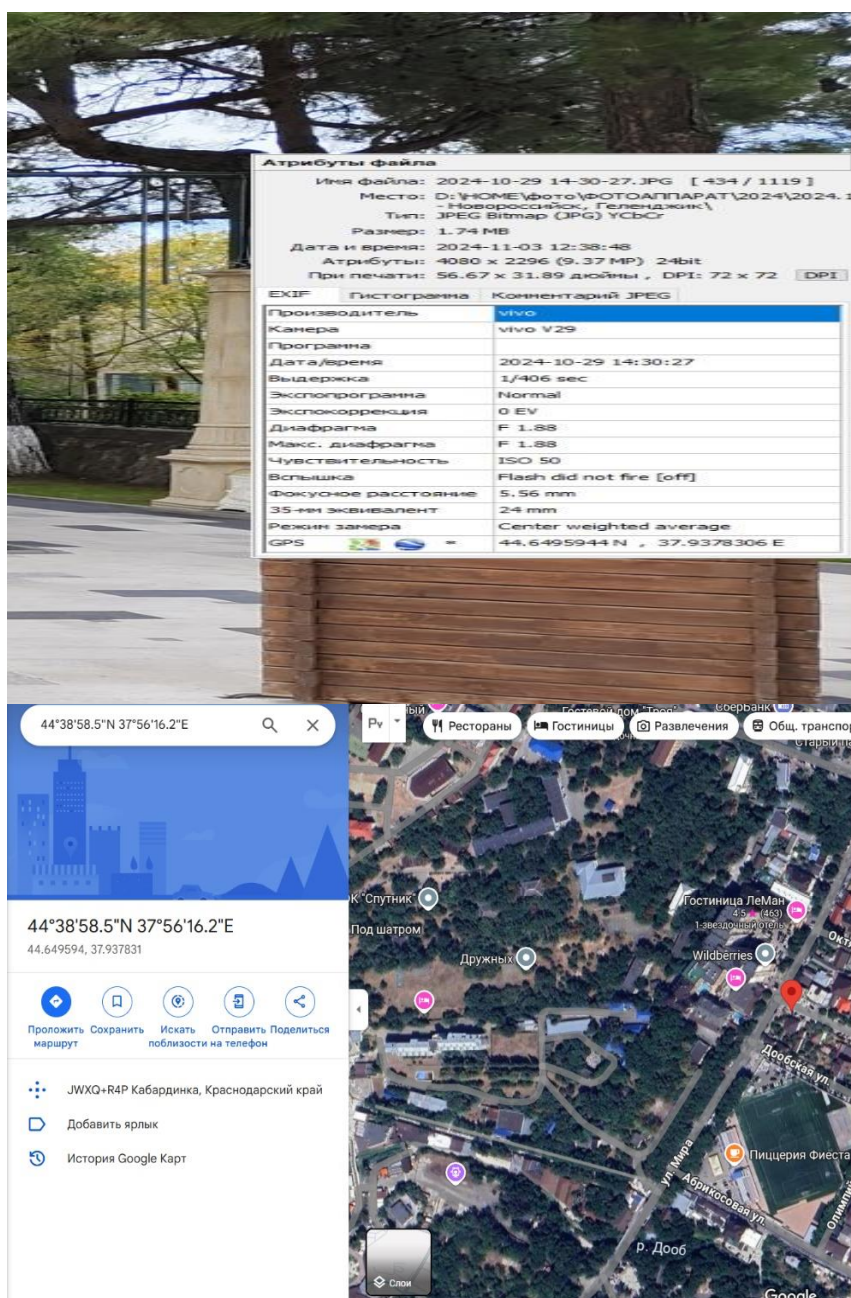
Однако не всегда на личной странице разыскиваемого лица имеется реальная фотография, поэтому необходимо использовать иные методы поиска конкретного человека. Это можно сделать путем анализа активности IP, либо MAC адреса устройства, проверки общих знакомых лица, участие в группах и т.д.

Кроме поиска лиц можно искать места, похищенные предметы, транспортные средства и иные объекты, изображенные на фотографии: в Яндекс («Панорамы и фотографии», «Зеркала») и Google («Просмотр улиц»).

Анализ фотографий (EXIF)

При анализе фотографии, загруженной пользователем в сеть Интернет, необходимо изучить метаданные EXIF (Exchangeable Image File Format), которые хранятся в самом начале самих файлов фотографий (до данных фактического изображения). По этим данным можно определить:

- название и версию программного обеспечения (камеры);
- дату и время съемки;
- данные о цифровой среде;
- географические координаты местоположения; ориентация камеры (вертикальная или горизонтальная);
- размер матрицы;
- информация об авторе и т. д.



Наибольший интерес представляют данные о местоположении сделанного снимка. Также отметим, что EXIF легко поддаётся редактированию.

Существуют онлайн-сервисы для изменения съёмочных параметров, поэтому данные EXIF могут выступать ориентирующей и справочной информацией.

Для просмотра EXIF – информации можно воспользоваться бесплатной программой FastStone Image Viewer (<https://faststone.org>).

Информация по IP-адресу, DNS

Для определения оператора сотовой связи, провайдера, предоставляющего услуги доступа в сеть Интернет по известному IP - адресу можно воспользоваться сервисами <https://2ip.ru/whois>. Кроме того, можно получить информацию о стране, которой по данным «RIPE Database query service» данный адрес выдан, населенном пункте, часовом поясе, диапазоне IP-адресов провайдера, подсети (CIDR-блок), маршрутах трафика (BGP), PTR-записях (обратное DNS-имя).

На сайте <https://whois.ru> можно получить данные о владельце домена и его контактную информацию, IP-адреса сайта, дате регистрации, компании-регистраторе, компании и месторасположению хостинга, истории DNS-записей и т. д.

Мессенджеры Telegram, WhatsApp

Для поиска информации по мессенджерам рекомендуется использовать веб-версию соответствующего мессенджера на стационарном компьютере (на примере Telegram).

1. Поиск пользователя осуществляется путем встроенного поиска Telegram (@username или ключевые слова), сторонних сервисов, таких как <https://tgstat.ru> и <https://telemetr.io>, либо с использованием поисковой системы Яндекс [site:t.me «ключевое слово»](https://yandex.ru/search/?text=t.me%20ключевое%20слово).

2. В открытых группах можно извлечь информацию о подписчиках, а также провести анализ сообщений участников, их активности.

3. Парсинг постов и метаданных с использованием ботов (@GetInfoBot, @SangMata_info_bot), сканирование через API (<https://github.com/LonamiWebs/Telethon>, <https://github.com/pyrogram/pyrogram>).

4. Использование @userinfobot и @SangMata_info_bot для сбора истории изменений имени.

5. Боты для анализа медиафайлов: @ExifToolBot – проверка метаданных изображений, @pic2map_bot – проверка геолокации фото.

6. Поиск по аватару (фотографии) и никнейму лица в сети Интернет.

7. Исследование метаданных файлов, опубликованных пользователем.

8. Просмотр никнейма, истории и аватара по номеру телефона путем перехода по ссылке <https://t.me/+7908133559>* (последняя цифра скрыта нами).

Деанонимизация лица по номеру телефона

По номеру телефона можно получить персональные данные лица с использованием приложения «GetContact». Основные возможности:

- узнать, как записан номер в контактах у других пользователей;
- определить возможные связи и ассоциации по тега;
- определить род деятельности (если присутствуют теги вроде «Мария Автострахование»).

Для использования программы можно скачать официальное приложение из Google Play или App Store, зарегистрироваться и проверить номер. При наличии подписки можно посмотреть больше тегов. Данный способ рекомендуется использовать только с виртуальной или временной сим-картой,

то есть не связанной с персональными данными сотрудника правоохранительных органов.

Веб-поиск

1. Поиск упоминаний номера телефона на сайтах сети Интернет с использованием поисковых систем.
2. Формирование списка релевантных сайтов и страниц для последующего парсинга.
3. Переход и изучение найденных страниц с использованием языка поисковых запросов Яндекса (ограничение поиска по конкретному домену).

Поиск по социальным сетям

1. Внесение телефона разыскиваемого лица в адресную книгу телефона.
2. Синхронизация контактов социальной сети и телефонной книги, включение настроек поиска друзей по телефонной книге в настройках приложения («ВКонтакте», «Одноклассники»).
3. Отображение лица в «рекомендуемых друзьях».

Поиск в мессенджерах

1. Проверка регистрации в мессенджерах. Для этого в браузере указывается ссылка следующего формата: https://t.me/+7908133559*.
2. Установка ID пользователя с помощью специальных телеграм-ботов (@username_to_id_bot, @CheckID_AIDbot).
3. Установка даты создания учетной записи с помощью бота @creationdatebot.
4. Поиск сведений о пользователе в базах данных деанонимизированных пользователей Telegram, к примеру, @UwU_DDUVRD_bot, @Mervervar_Bot.
5. Проверить присутствие пользователя в Telegram и его круг интересов с помощью @telesint и @eyeofbeholder_bot.
6. Получить данные об активности и упоминаниях пользователя с помощью специальных поисковых систем <https://lyzem.com>.
7. Установление аккаунтов на иных ресурсах (социальных сетях, игровых сайтах, форумах), которые зарегистрированы с никнеймом, тождественным username устанавливаемого пользователя. Возможными способами решения этой задачи являются: точный (с использованием кавычек) поиск в Google и Yandex, целевой поиск соответствующих никнеймов на ресурсах, в которых предполагается присутствие искомого пользователя, применение специальных инструментов и сервисов, выполняющих быстрый поиск по никнеймам на сотнях ресурсов (бот @maigret_osint_bot, веб-сервисы <https://suip.biz/ru>, <https://namechk.com>).
8. Проанализировать все сообщения от пользователя в чатах Telegram, в которых он состоит. Нередко лица в сообщениях оставляют текстовую, графическую, звуковую или видеоинформацию, которая прямо или косвенно может способствовать их идентификации.
9. Вступив в группу, в которой состоит интересующий нас пользователь, можно выгрузить историю сообщений с помощью функции «Экспорт истории чата» (она доступна в десктопной версии Telegram). Для анализа этой истории лучше всего использовать программу «Архивариус 3000», которая позволяет выискивать в переписке такие сущности, как номер телефона, адреса электронной почты, URL, IP-адреса, а также считать частоту

их использования. Весьма полезная вещь, которая нередко помогает находить забытые авторами сообщений ссылки на свои блоги и личные кабинеты, давно потерянные контакты и страницы в социальных сетях.

10. При размещении пользователем изображений (как в качестве аватара, так и в виде фотоизображений в сообщениях) могут применяться инструменты поисковых систем, но лучший результат дают ресурсы, специализирующиеся на поиске по фото, к примеру, <https://pimeyes.com/>, <https://tineye.com/>, <https://search4faces.com>.

11. Поиск по изображениям местности, интерьерам, частям тела, одежде и аксессуарам.

12. Ссылки-ловушки. При переходе по подобной ссылке, посланной под каким-либо предлогом устанавливаемому пользователю, инициатору становится известен IP-адрес и некоторые другие данные об используемом устройстве и программном обеспечении. Наиболее известными онлайн - сервисами по созданию ссылок ловушек являются <https://iplogger.ru/> и <https://grabify.link/>.

Просмотр удаленных страниц

Если нужно посмотреть удалённые страницы в Интернете, есть несколько способов.

1. Использование веб-архивов. Wayback Machine (web.archive.org) –самый крупный интернет-архив, позволяет просматривать сохранённые версии сайтов по дате.

2. Google Cache. Если страница недавно удалена, её копия может быть в кэше Google. Вставить в поисковую строку Google: `cache:site.com/page`.

3. Поиск через поисковые системы. Google Dorking (поиск по следам) – если страница удалена, но её копии есть в сети.

Парсинг сайтов (web scraping)

Парсинг (web scraping) – это процесс автоматического сбора данных с веб-страниц сети Интернет. Он может быть использован для поиска криминалистически значимой информации, выявления мошенников, собирания доказательств и мониторинга ресурсов сети Интернет.

Выделяют 2 формы парсинга.

1. Статический парсинг используется для поиска и извлечения информации с веб страниц, которые формируются на стороне сервера. К наиболее распространённым способам осуществления такого парсинга относят использование библиотек Python: Requests (<https://github.com/psf/requests>), BeautifulSoup (<https://beautiful-soup.readthedocs.io/en/latest>).

2. Динамический парсинг используется для сайтов, загружающих данные через JavaScript и требует эмуляции браузера. Наиболее распространенная библиотека Python – Selenium (<https://github.com/SeleniumHQ/Selenium>).

К универсальным типам программ для осуществления парсинга, а также автоматизации любых действий в браузере можно отнести Browser Automation Studio (<https://bablosoft.com/shop/BrowserAutomationStudio>).

К основным возможностям программы можно отнести следующие:

- автоматизация работы в браузере;
- вход на сайты по логину и паролю;
- заполнение форм и отправка данных;
- клики, скроллинг, нажатие клавиш;

- парсинг веб-страниц;
- извлечение данных из HTML-кода;
- сохранение информации в файлы;
- обход CAPTCHA;
- работа с прокси-серверами и анонимностью;
- подмена User-Agent и скрытие следов в сети;
- подключение к сервисам (например, Telegram API, VK API);
- отправка и получение данных через HTTP-запросы;
- поиск данных (email, пароли);
- управление сессиями и куками.

Специализированные программы могут помочь собрать различные типы данных с целевого сайта. Одним из таких инструментов является Harvester (<https://github.com/laramies/theHarvester>), который осуществляет поиск и извлекает следующую информацию с сайта: адреса электронной почты, личные данные пользователей и т. д. Данная информация может быть собрана из различных источников, таких как Google, Yandex и т. д.

Анализ текста

Для анализа, поиска и систематизации больших объемов текста, полученного путем парсинга, экспорта переписки в какой-либо группе, используются различные программы и инструменты, которые помогают эффективно работать с большими данными. Эти инструменты можно условно разделить на несколько категорий в зависимости от их назначения и функциональности.

Для работы с документами в различных форматах (PDF, DOC, TXT) можно использовать программу DocFetcher (<https://docfetcher.sourceforge.io/ru/index.html>), которая позволяет индексировать и быстро искать текст в больших наборах документов.

«Архивариус 3000» – это программа для поиска документов и почтовых сообщений на компьютере, в локальной сети и на съемных носителях. Поиск осуществляется по ключевым словам или с использованием языка запросов, аналогичного поисковым системам.

Программа извлекает и сохраняет полную информацию о документах, что позволяет находить и просматривать файлы даже в случае их физической недоступности. Встроенные инструменты обеспечивают быстрый просмотр и печать документов, а также удаленный поиск и доступ к файлам через интернет.

«Архивариус 3000» поддерживает работу со всеми популярными форматами документов, включая файлы MS Office, PDF, TXT и LEX. Возможен поиск внутри архивов (ZIP, RAR, ARJ и другие), а также в почтовых сообщениях Outlook, Outlook Express, The Bat! и вложенных в письма документах.

Основные функции:

- быстрый полнотекстовый поиск документов и электронной почты;
- смысловой поиск с морфологическим анализом на 18 языках;
- поддержка работы в локальной сети и на съемных дисках;
- совместимость с форматами MS Office, PDF, TXT, LEX;
- поиск данных внутри архивов ZIP, RAR, ARJ и других;
- анализ почтовых сообщений из Outlook, Outlook Express, MS Exchange, The Bat! и других почтовых клиентов;

- возможность поиска в базах данных Lotus Notes и Lotus Domino;
- серверный режим с доступом к рабочим документам через Интернет;
- полная поддержка кодировки Unicode.

2. Инструменты для анализа больших объемов текста. Для более глубокой обработки и анализа текстов на естественном языке популярны библиотеки для программирования, такие как NLTK (<https://www.nltk.org>) и spaCy (<https://spacy.io>). Эти библиотеки используются для обработки и анализа текстов, поиска ключевых слов, анализа частотности слов, а также для более сложных задач, таких как анализ смысловых связей и извлечение информации.

Кроме того, для обработки больших текстовых данных и создания поисковых систем часто используются Apache Solr (<https://solr.apache.org>) и Elasticsearch (<https://www.elastic.co/elasticsearch>). Эти системы обеспечивают быстрый поиск по текстам и позволяют индексировать огромные объёмы информации, что делает их полезными для поиска в больших коллекциях документов.

Также существует онлайн-инструмент Voyant Tools (<https://voyant-tools.org>), который предоставляет различные способы для анализа текста, включая подсчёт частоты слов и создание визуализаций для лучшего понимания структуры и содержания текста.

3. Систематизация и управление текстовой информацией. Эти инструменты помогают организовывать и управлять текстовой информацией.

Obsidian – программа для ведения заметок с возможностью создания связей между текстами.

Базы знаний (работа с Big Data)

Obsidian (<https://obsidian.md>) – инструмент для создания, организации и управления заметками, предназначенный для ведения базы знаний. Программа позволяет эффективно работать с отдельными категориями информации путем создания корреляционных взаимосвязей в виде графов знаний. К основным возможностям можно отнести следующие:

- создание ссылки между отдельными фактами, что помогает организовывать информацию в виде взаимосвязанной сети;
- автоматическое построение графа взаимосвязей с визуализацией структуры базы знаний;
- язык разметки Markdown для форматирования текста;
- локальное хранение данных;
- поддержка установки множества плагинов, расширяющих функциональность (календарь, таблицы, диаграммы, скрипты и другие).
- мгновенный полнотекстовый поиск по всему хранилищу заметок;
- возможность использования сложных поисковых запросов для быстрого нахождения нужной информации;
- поддержка тегов, категорий;
- создание сложных систем категоризации с помощью ссылок и вложенных структур;
- интеграция с другими сервисами и базами данных.

Онтология

Онтология представляет собой формальное описание понятий в рассматриваемой предметной области (классов), свойств каждого понятия, его атрибутов (слов, иногда их называют ролями) и ограничений, наложенных на слоты (фацетов, иногда их называют ограничениями ролей). Онтология вместе

с набором индивидуальных экземпляров классов образует базу знаний. Наиболее распространённым и универсальным редактором онтологий является программа Protégé (<https://protege.stanford.edu>).

Использование данного программного продукта является бесплатным и доступно в 2 формах: как отдельная программа и как web-приложение, запускаемое в браузере. Функционал указанных решений во многом схож, однако настольная версия содержит в себе больше возможностей.

Онтология предполагает определение любых понятий и сущностей предметной области во взаимосвязи трех элементов: субъект-предикат- объект (такой элемент часто называют триплетом). Совокупность триплетов образует граф понятий. Субъекты и объекты интерпретируются как вершины ориентированного графа, а предикаты определяют отношения между сущностями. В отдельных случаях предикат (отношение, корреляционная связь) может быть субъектом или объектом в рамках другого графа.

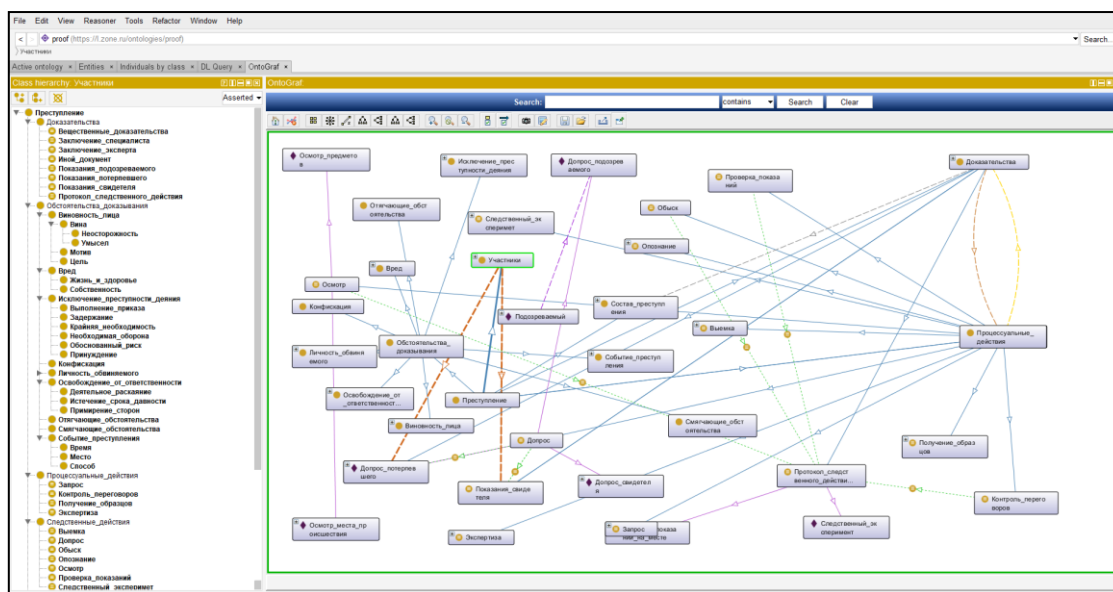


Рис. 1 Визуальное представление категории «Обстоятельства, подлежащие доказыванию»

Для создания онтологии расследования мы сформировали следующие корневые классы:

- 1) Доказательства;
- 2) Обстоятельства_доказывания;
- 3) Процессуальные_действия;
- 4) Следственные_действия;
- 5) Состав_преступления;
- 6) Участники.

Каждый элемент корневого класса имеет вложенные классы (subclasses), которые с помощью отношений или выражений имеют корреляционную связь с одним или несколькими вложенными классами другого корневого класса. К примеру, корневой класс «Состав_преступления» содержит следующие вложенные классы:

- 1) Объект (также содержит вложенные классы: жизнь, здоровье, собственность и т. д.);
- 2) Объективная_сторона (вложенные классы: время, место, способ);

- 3) Субъект (вложенные классы: вменяемость, возраст);
- 4) Субъективная сторона (вложенные классы: вина, мотив, цель).

Каждый класс имеет экземпляры, причем отдельный экземпляр может одновременно относиться к нескольким классам. Все классы (в том числе вложенные) связаны как между собой, так и с отдельными экземплярами класса с помощью отношений, выражений и скалярных констант. Среди отношений нами были сформированы следующие: «связан», «формирует», «устанавливает». Скалярные константы определяют весовые коэффициенты обстоятельства или вида доказательств. Такая взаимосвязь позволяет проследить корреляционные связи практически для любого экземпляра классов с учетом предложенных нами ранее коэффициентов и получить на основе анализа новые, не зафиксированные в процессуальных документах данные.

Приведем наглядный пример. По уголовному делу имеется доказательство – протокол осмотра места происшествия, в ходе которого обнаружены следы преступления и изъяты вещественные доказательства. Протокол является экземпляром нескольких классов:

- корневой класс – следственное_действие, вложенный класс – осмотр, так как в соответствии с УПК РФ осмотр места происшествия относится к виду осмотра, являющегося следственным действием;
- корневой класс – доказательства, вложенный класс – протокол_следственного_действия, вещественные_доказательства;
- корневой класс – обстоятельства_доказывания, вложенный класс – событие_преступления, вложенные классы – место, способ;
- корневой класс – состав_преступления, вложенный класс – объективная_сторона, вложенный класс – место_преступления;

Все указанные вложенные классы имеют определённый приоритет (силу), который умножается на коэффициент экземпляра класса, и в зависимости от решаемых задач выстраивается определённая онтология в определённом контексте. Очень упрощенно взаимосвязь осмотра места происшествия с иными элементами доказывания представлена на рисунке 2.

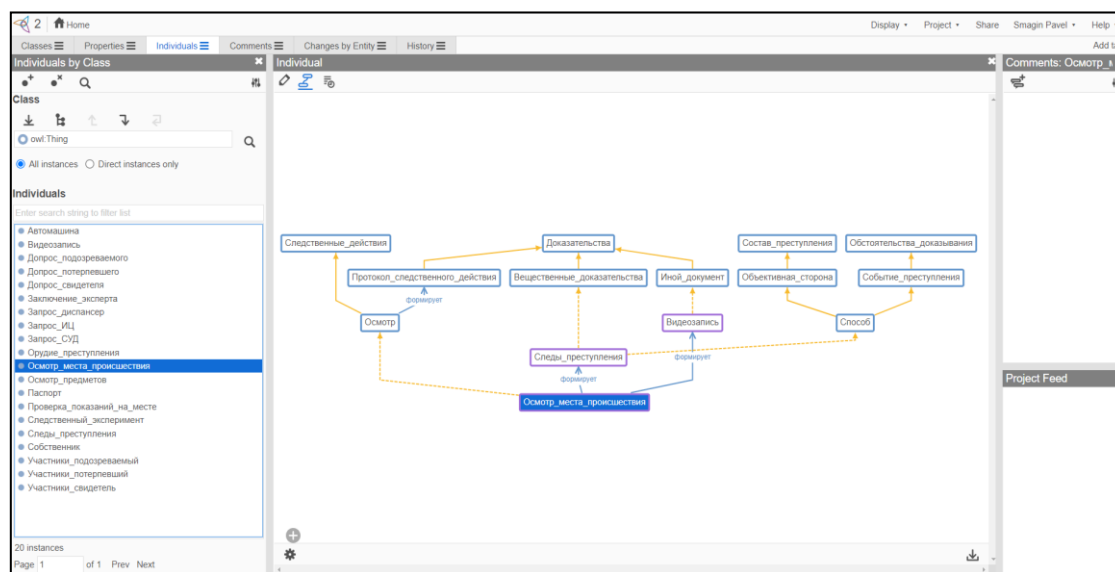


Рис. 2 Web-версия визуализации категории «Осмотр места происшествия»

Экспертная система, построенная на принципах онтологии, в контексте настоящего исследования позволяет решать следующие задачи:

- создание четкой структуры классов и категорий уголовно-процессуальных сущностей, позволяющих выстраивать иерархию с вложенными элементами и упрощающих понимание теории доказывания;
- выстраивание логической взаимосвязи между обстоятельствами, подлежащими доказыванию (установлению) и конкретными доказательствами, имеющимися в уголовном деле;
- создание корреляционных связей между свойствами доказательств, предметом и пределами доказывания;
- упрощение процесса планирования расследования, а также выдвижения и проверки версий;
- получение новой доказательственной и ориентирующей информации на основе логического анализа уже имеющейся информации;
- оказание консультативной помощи субъекту расследования для принятия обоснованных и аргументированных решений.

Использование нейросетей

Применение нейросетей в процессе раскрытия и расследования преступлений может решить следующие задачи.

1. Распознавание. Включает в себя определение ключевых признаков в анализируемых данных, таких как идентификация человека на основе внешности, распознавание номеров автомобилей или выявление определенных генетических последовательностей в геноме. Данная задача решается путем сопоставления объекта, представленного в системе, с ранее определёнными характеристиками.

2. Предсказание. Включает в себя определение будущего состояния информационной системы или ее отдельных параметров, таких как предсказание изменений уровня преступности. Система анализирует статистические данные и делает предположения о будущих событиях и развитии данных источников.

3. Классификация. Заключается в разделении данных на категории в соответствии с заранее заданными параметрами. Примеры включают в себя классификацию подписей как подлинных или поддельных или определение должника как недобросовестного.

Следователю в своей профессиональной деятельности приходится решать широкий спектр задач, связанных с анализом фотографий, видеозаписей, текстовой информации, в связи с чем для повышения эффективности решения указанных задач он может использовать предложенный нами алгоритм использования моделей машинного обучения как с использованием облачных решений, так и на своем **локальном компьютере**, что позволяет работать с информацией ограниченного доступа (служебной тайной).

1. **Google Colab** представляет собой бесплатную интерактивную облачную среду (блокнот) для работы с кодом на языке Python от Google в браузере. Сервис хорошо задокументирован на русском языке https://colab.research.google.com/notebooks/intro.ipynb?hl=ru_RU. Сообщество пользователей создало большое количество готовых блокнотов для решения широкого спектра задач, и для их использования не требуется знание языков программирования. Блокноты можно копировать в свой аккаунт,

систематизировать по папкам и запускать для решения конкретной задачи по мере необходимости.

Работа следователя с Google Colab сводится к следующим этапам:

- поиск и выбор блокнота через поисковую систему для решения конкретной задачи. К примеру, запрос может быть сформулирован так: «блокнот Google Colab для сегментации изображений» или «jupyter распознавания голоса из звукового файла». Jupyter — это расширение файла блокнота, который можно запустить в облачной среде;

- построчный запуск кода в блокноте. От пользователя требуется нажимать в порядке очередности код кнопкой, расположенной слева от кода. Многие блокноты содержат комментарии к коду в виде разметки *markdown*, в связи с чем понятно, в какую ячейку необходимо загрузить датасет (к примеру, для дообучения модели), а какая ячейка отвечает за формирование конечного результата.

- сохранение полученного результата в необходимой форме (таблица, график, диаграмма, фотография, звуковой или видеофайл).

К преимуществам Google Colab можно отнести: бесплатное использование мощных удаленных сервисов Google, скорость сети Интернет до 1Гб, предоставление в аренду специализированной видеокарты с тензорными ядрами для ускорения процесса обработки данных. Однако у рассмотренного подхода имеются и минусы: невозможность обрабатывать информацию с ограниченным доступом, наличие сети Интернет для доступа к блокноту.

Аналогом Google Colab на локальном компьютере может выступить Jupyter Notebook (в пакете Anaconda), работающий на Python.

2. Платформа *Hugging Face* (<https://huggingface.co>) содержит коллекцию готовых предварительно обученных моделей глубокого обучения (концепция Deep Learning). Сервис использует библиотеку Transformers (распространяется под лицензией Apache License 2.0), предоставляющую инструменты и интерфейсы для загрузки, использования и дообучения моделей. Документация библиотеки доступна на русском языке по адресу: <https://huggingface.co/learn/nlp-course/ru>.

Трансформеры — относительно новый тип нейросетей, направленный на решение последовательностей с обработкой дальнедействующих зависимостей. Основными компонентами трансформеров являются энкодер и декодер. Энкодер преобразовывает входящую информацию (например, текст) и с помощью токенайзера (словаря) конвертирует ее в векторное представление в виде эмбедингов (наборов чисел). Декодер, в свою очередь, расшифровывает ее в виде новой последовательности (например, ответ на вопрос).

Трансформеры реализуют концепцию взаимосвязи 3 сущностей:

- позиционные энкодеры (Positional Encodings) и декодеры;
- внимание (Attention);
- самовнимание (Self-Attention).

Модели Transformers поддерживают три фреймворка: PyTorch, TensorFlow и JAX. Библиотека Transformers не является набором модулей, из которых формируется нейронная сеть, как например PyTorch, а представляет собой несколько высокоуровневых абстракций, которые позволяют работать с моделями в несколько строк кода.

Сервис Hugging Face позволяет использовать готовые модели машинного обучения в нескольких формах в зависимости от выбора задачи и облачного

запуска виртуальной среды для ее решения (<https://huggingface.co/tasks>). Список задач достаточно обширный и включает в себя несколько категорий.

Hugging Face поддерживает широкий спектр задач машинного обучения, включая обработку текста, изображений, аудио и многомодальные модели.

1. NLP (Natural Language Processing) – обработка текста:

- текстовая классификация (анализ тональности, определение темы);
- распознавание именованных сущностей (NER);
- автоматическое краткое изложение текста (Summarization);
- генерация текста (GPT, Llama, Mistral и др.);
- машинный перевод (Machine Translation);
- преобразование текста в текст (Text-to-Text, T5, BART);
- ответы на вопросы по тексту (Question Answering);
- анализ слов в тексте (Token Classification);
- поиск похожих текстов (Text Similarity, Semantic Search);
- представление текста в векторной форме (Text Embeddings).

2. Computer Vision – обработка изображений:

- классификация изображений (Image Classification);
- обнаружение объектов (Object Detection, YOLO, DETR);
- сегментация объектов (Image Segmentation);
- генерация описаний к изображениям (Image-to-Text, BLIP, CLIP);
- генерация изображений (Stable Diffusion, DALL-E);
- улучшение качества изображений (Super Resolution);
- распознавание лиц (Face Recognition).
- распознавание текста на изображениях (OCR).

3. Speech Processing – обработка аудио:

- распознавание речи (ASR, Whisper, Wav2Vec);
- генерация голоса из текста (Text-to-Speech, TTS);
- определение эмоций по голосу (Speech Classification);
- идентификация говорящего (Speaker Identification);
- изменение голоса (Voice Conversion);

4. Multimodal – обработка различных типов данных:

- модели для работы с изображениями и текстом (Vision-Language Models, CLIP, Flamingo);

- генерация описаний к картинкам (Image Captioning);
- ответы на вопросы по изображениям (Multimodal Question Answering).

5. Таблицы и структуры данных:

- ответы на вопросы по таблицам (Table Question Answering, TAPAS, T5);
- анализ сложных документов (Document AI, LayoutLM, Donut);
- извлечение информации из данных (Information Extraction).

Большую часть моделей можно запустить на локальном компьютере.

Выделим **направления** их использования в деятельности следователя:

1. Получение (парсинг — автоматизированный сбор и систематизация информации из открытых источников с помощью скриптов) и обработка общедоступной информации сети Интернет. Среди таких задач отметим:

- поиск изображений по словесному описанию на определенном сайте (к примеру, похищенные предметы среди объявлений о продаже на электронных торговых площадках);

- выявление объявлений о продаже запрещенных в гражданском обороте предметов с измененным описанием (продажа травматического и газового оружия на маркетплейсах под видом сувениров и игрушек);

- анализ поведенческих факторов и личных характеристик пользователя по оставленным им комментариям в открытых источниках (к примеру, видеохостингах и форумах);

- поиск криминалистически значимой информации на фотографиях и видеозаписях, размещенных в открытом доступе в сети Интернет;

- выявление преступлений в области нарушений авторского права;

- анализ судебных решений для раскрытия преступлений прошлых лет, имеющих аналогичный способ совершения, номера телефонов, адреса, марки и номера транспортных средств и т. д.

- формирование методик расследования преступлений на основе анализа криминалистической характеристики преступлений [8].

2. Обработка больших объемов текстовой информации для их классификации по категориям и извлечения определённых признаков. Указанный подход позволяет установить пострадавших от преступлений, которые не обращались в органы внутренних дел, однако заявляли о преступлении в сети Интернет (например, потерпевших от мошенников или организаторов финансовых пирамид).

3. Получение и анализ текста из аудио- и видеозаписей, не содержащих информацию ограниченного доступа.

4. Обработка видеозаписей с общедоступных камер видеонаблюдения с целью выявления латентных преступлений, определения способов движения транспорта и лиц, причастных к совершению преступлений.

К минусам облачных сервисов Hugging Face и Google Colab можно отнести ограничения, связанные с конфиденциальной информацией (служебная тайна, персональные данные, врачебная, банковская, налоговая тайны и т. д.), в связи с чем рассмотрим возможности работы с моделями машинного обучения в локальной среде.

Расширения для браузера

Расширения для браузера для целей OSINT.

1. Wappalyzer определяет технологии, использованные на веб-сайтах, например, платформы для создания сайтов, системы управления контентом (CMS), веб-серверы, аналитические сервисы и другие.

2. Shodan позволяет искать устройства и серверы, подключенные к интернету, через платформу Shodan.

3. Hunter.io – инструмент для поиска адресов электронной почты, связанных с определенным доменом.

4. Social Search – расширение для поиска людей в различных социальных сетях, таких как Facebook, LinkedIn, Twitter и других по имени или другим данным.

5. Wayback Machine доступ к архивам старых версий веб-сайтов через Internet Archive. Полезно для изучения изменений на сайте в разные временные периоды.

Открытые базы данных

Помимо информации, размещаемой пользователями в открытых источниках, можно отнести сайты государственных и муниципальных органов, которые публикуют информацию посредством сети Интернет в соответствии с

нормативными правовыми актами. Перечень таких сведений предусмотрен Федеральным законом «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»¹ и распоряжением Правительства Российской Федерации от 10 июля 2013 г. №1187-р².

Приведем лишь малую часть таких сервисов. Так, на сайте главного управления по делам миграции (<http://services.fms.gov.ru/index.htm>) можно осуществить проверку недействительных российских паспортов, действительности разрешений на работу и патентов на осуществление трудовой деятельности иностранными гражданами и лиц без гражданства, соответствие документа и адреса регистрации. На сайте федеральной налоговой службы (<https://service.nalog.ru/inn.do>) можно узнать индивидуальный номер налогоплательщика (ИНН). На сайтах судов можно посмотреть участников уголовного и гражданского судопроизводства. На сайте федеральной налоговой службы (<https://service.nalog.ru/inn.do>) сведения о наличии в отношении лица исполнительных производств и нахождение лица в розыске. На сайте Росреестра можно получить сведения о собственниках недвижимого имущества: https://rosreestr.gov.ru/eservices/request_info_from_egrn. Судебные решения, приговоры и иные судебные акты публикуются на сайтах судов и сайте <https://sudact.ru>. С перечнем террористов и экстремистов можно ознакомиться на сайте <http://fedsfm.ru/documents/terrorists-catalog-portal-act>. Единая база ОСАГО (сведения о действительных полисах в привязке к автомобилю) находится по адресу: <https://nsis.ru>. Сведения о штрафах в области безопасности дорожного движения: <https://гибдд.рф/check/fines>. Реестр уведомлений о залогах имущества: <https://www.reestr-zalogov.ru/search/index>. Единый государственный реестр юридических лиц: <https://egrul.nalog.ru>. Реестр недобросовестных поставщиков: <http://zakupki.gov.ru/epz/dishonestsupplier>. Сведения о деятельности юридических лиц: <http://www.fedresurs.ru>.

Установление стоимости похищенных предметов

В процессе проверки сообщения о преступлении нередко у следователя возникает необходимость установления предварительной оценки стоимости похищенного имущества. Необходимо это в случаях отсутствия документов на похищенное, явное завышение или занижение размера причиненного ущерба. Рекомендуются для определения среднерыночной цены воспользоваться электронными торговыми площадками по продаже товаров. К примеру, для установления стоимости автомашины можно воспользоваться сайтом <https://auto.ru>. После введения сведений о похищенной автомашине (год, комплектация, цвет и т. д.) можно узнать информацию о среднерыночной стоимости автомобиля. Эта информация будет ориентировочной, но она поможет квалифицировать преступление.

¹ Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления : Федеральный закон от 09.02.2009 №8-ФЗ // СПС «КонсультантПлюс».

² О Перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети Интернет в форме открытых данных : распоряжение Правительства РФ от 10.07.2013 № 1187-р // СПС «КонсультантПлюс».

Все 30

С пробегом 30

Новые

Каталог

Отзывы

Тест-драйвы

BA3 (Lada)

Kalina

Поколение

+

Кузов

Коробка

Двигатель

Привод

Объем от, л

до

2010

2010

Пробег от, км

до

Цена от, руб.

до

Воронеж + 200 км

Все параметры

Сбросить

30 объявлений

Сохранить поиск

По актуальности

За все время

Р

С фото

			
BA3 (Lada) Kalina I 2010, 78 000 км седан, серебристый 1.6 MT (81 л.с.) бензин, передний	BA3 (Lada) Kalina I 2010, 120 000 км хэтчбек 5 дв., серебристый 1.6 MT (81 л.с.) бензин, передний	BA3 (Lada) Kalina I 2010, 86 000 км универсал 5 дв., серебристый 1.4 MT (89 л.с.) бензин, передний	BA3 (Lada) Kalina I Sport 2010, 54 000 км, KIA Центр - ... хэтчбек 5 дв., чёрный 1.4 MT (89 л.с.) бензин, передний
Урюпинск	Белгород	Воронеж	Липецк
205 000 Р	210 000 Р	225 000 Р	250 000 Р

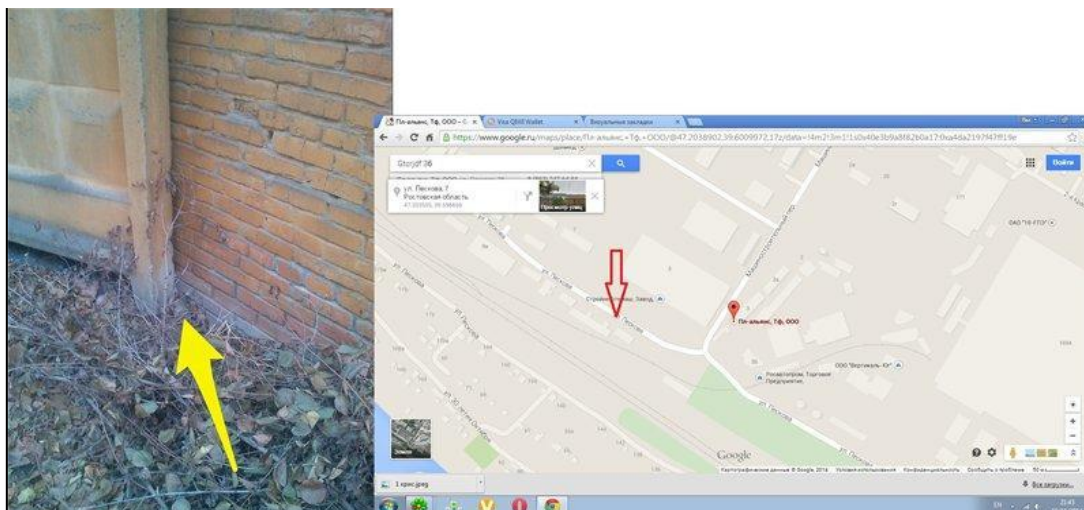
Выявление преступлений

Незаконный оборот наркотических средств

Сеть Интернет является в настоящее время очень востребованным в криминальных структурах средством для осуществления незаконной «торговой» деятельности различными предметами и веществами, которые запрещены к свободному гражданскому обороту. В первую очередь это касается распространения наркотических средств и оружия.

Существует несколько схем использования сети Интернет при распространении наркотических средств, но все они действуют по схожему принципу. Создается группа в мессенджере, сообщество в социальной сети, в которых размещаются инструкции, реквизиты для оплаты, ассортимент «товаров» и расценки на них. С помощью сарафанного радио группа быстро обретает популярность в среде лиц, употребляющих наркотические средства. Зачастую такие ресурсы не содержат словосочетаний, которые позволили бы отнести размещенную на сайте информацию к пропаганде и распространению наркотических средств. К примеру, героин на сленге называют белый, главный, коричневый, лекарство, перец, султан, хлеб; марихуану – гарик, марго, дым, молоко, пластилин, трава, шишки, план и т. д.

После оплаты лицу высылается инструкция о местонахождении «закладки» с наркотическим средством. Сделано это может быть как с использованием сайта, так и посредством сообщения в одном из мессенджеров.



Сам процесс выявления указанных ресурсов и их владельцев может осуществляться по нескольким направлениям. К первому можно отнести традиционные способы. К примеру, задержанный за немедицинское употребление наркотических средств в своих показаниях указывает группу в мессенджере «Телеграм», посредством которой он приобретал наркотические вещества, либо ресурс становится известен правоохранительным органам путем проведения мониторинга и аналитической работы.

Преступления против собственности

Мошенничества с использованием сети Интернет занимают значительную долю в статистике совершения преступлений.

На тематических форумах, в группах социальных сетей «ВКонтакте», «Одноклассники» мошенники представляются сотрудниками банков (как правило, Сбербанка) и путем обмана выясняют у граждан личные данные для входа в онлайн версии банков. К примеру, для того чтобы зайти в Сбербанк-онлайн, требуется знать логин (идентификатор) лица и подтвердить перерегистрацию на мошенника, сообщив последнему лишь код из СМС. Далее мошенник быстро переводит доступные в личном кабинете деньги на другие счета.

Для выявления указанных преступлений сотрудникам правоохранительных органов необходимо активно взаимодействовать с администрациями тематических сайтов и модераторами групп. С этой целью направляются официальные запросы, которые позволяют установить IP-адреса мошенников и их местонахождение.

Достаточно часто преступления совершаются с использованием досок объявлений. В частности, посредством сайта «Avito» (<https://www.avito.ru>) мошенники путем обмана вынуждают потерпевших переводить деньги на свои пластиковые карты либо пополнить счет телефона, после чего на связь не выходят.

Приведем пример. Лицо выставляет на продажу какой-либо товар по цене значительно ниже рыночной. При разговоре с потенциальным покупателем мошенник заявляет, что может «забронировать» данный товар для покупателя, но при этом просит перевести незначительную сумму для гарантии серьезных намерений покупки. После обмана нескольких человек мошенник обязательства не исполняет.

Для выявления указанных преступлений необходимо осуществлять мониторинг объявлений, размещенных на сайте «Авито», в первую очередь, с точки зрения их цены. Этого можно добиться путем использования специализированных парсеров сайтов, которые в автоматическом режиме будут сканировать все объявления.

Изготовление поддельных документов

При выявлении преступлений, связанных с изготовлением и использованием поддельных документов, поисковые системы позволяют установить сайты, на которых осуществляется продажа дипломов, водительских удостоверений, иных официальных документов.

Сотрудниками полиции в таком случае должен быть проведен комплекс оперативно-розыскных мероприятий, направленных на документирование фактов изготовления поддельных документов. Недолгий поиск таких сайтов позволил нам выявить несколько сайтов, на которых продаются дипломы.

**Диплом специалиста
выдается 2014**



Гознак: 2014

Цена: 24000 **19000**

**Аттестат о среднем
образовании**



Гознак: Любой год выпуска

Цена: 13000 **12 000**

**диплом
колледжа(техникума) с
2014**



Гознак:

Цена: 18000 **17 000**

**Академическая
справка**



Гознак:

Цена: 13000 **11 500**

**Диплом бакалавра
выдается с 2014**



Гознак: Гознак 2014 года

Цена: 24000 **19000**

**О профессиональной
подготовке**



Гознак: С 2004 года

Цена: 20000 **19 000**

Свидетельство о браке



Гознак:

Цена: 19000 **16 000**

**Диплом
техникума(колледжа)
2011-2013**



Гознак:

Цена: 18000 **16000**

Незаконные организация и проведение азартных игр

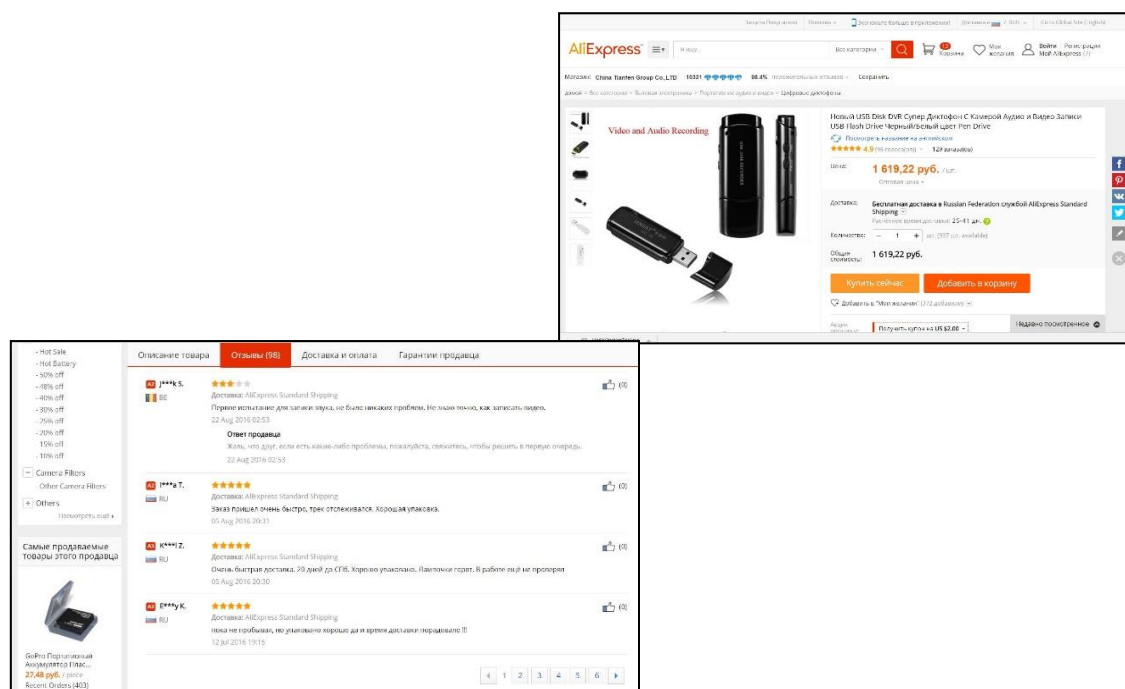
Аналогичная ситуация складывается и вокруг игровой деятельности. Не составляет большого труда установить сайты и их владельцев, которые занимаются указанной деятельностью.

Необходимо учитывать, что по адресу сайта не так сложно установить его администратора (лица, который этот сайт поддерживает). Это можно сделать через соответствующего провайдера, который путем анализа сетевого IP-адреса сможет предоставить информацию о точном местоположении правонарушителей.

Незаконный оборот специальных технических средств

Обращаясь к незаконному обороту специальных технических средств, следует сказать, что значительная часть технических средств приобретается через сеть Интернет. Так, на достаточно известном сайте

<https://ru.aliexpress.com/> можно без труда найти товары, приобретение которых влечет наступление уголовной ответственности.



К сожалению, взаимодействие с правоохранительными органами других стран, в частности Китая, в настоящее время оставлять желать лучшего, поэтому установить конкретных лиц, которые приобрели тот или иной товар, можно путем анализа отзывов, которые содержатся на странице карточки товара, либо путем взаимодействия с таможенной службой.

Нарушение авторских прав (торренты)

Во всем мире в наши дни проводится огромная работа по защите авторских прав, однако на большом количестве ресурсов в русскоязычном сегменте сети Интернет эти права нарушаются. Так, на наш взгляд, блокирование доступа к сайту для пользователей не всегда эффективно, так как многие сайты расположены в других странах и физически блокировать их работу невозможно, а многие пользователи обходят указанную блокировку с использованием прокси-серверов и VPN.

Более эффективным способом борьбы с нарушением авторских прав является установление владельцев торрент-сайтов и прекращение деятельности самого сайта.

Выявление мошенничеств при государственных закупках

Мошенничества в сфере экономической деятельности составляют достаточно большую долю преступлений, которые можно выявить, проводя анализ сведений, содержащихся в сети Интернет.

Как правило, преступления, касающиеся проведения торгов и аукционов, совершаются по следующей схеме: мошенник регистрирует компанию (например, ООО «Компания») и размещает на электронной торговой площадке аукцион на приобретение какого-либо товара. Сумма контракта зачастую составляет несколько миллионов рублей с ценой выше средней по рынку. Возможность проведения аукционов доступна не только органам власти по государственным закупкам, но и частным лицам. Наиболее распространенными

площадками являются Сбербанк-Аст (<http://www.sberbankast.ru/>) и Единая торговая площадка (<https://www.roseltorg.ru>).

Часто бывают ситуации, когда заказчик хочет заключить договор с конкретным, заранее определенным поставщиком. Например, если это поставщик, с которым ранее уже совершались успешные сделки, или некое аффилированное лицо. Бывает, что поставщик выходит на связь с сотрудником заказчика и предлагает вознаграждение за протекцию.

По закону заказчик обязан проводить открытую конкурентную процедуру закупки. Отклонять заявки других поставщиков он может только в том случае, если эти заявки не соответствуют требованиям закупочной документации.

Так, проводится закупка на монтаж и обслуживание пожарной сигнализации. В технической документации прописаны параметры оборудования, виды датчиков и т.п., а в проекте договора отдельно ещё указано, что тот же поставщик должен поставить компьютер для подключения системы с узко заданными характеристиками. Большинство поставщиков ориентировались только на описание оборудования, не заметив дополнительного требования про компьютер. В результате их заявки были отклонены как несоответствующие требованиям документации, и выиграл нужный поставщик.

Ещё один вариант использования невнимательности поставщика – это отформатировать документы с описанием требований к ТРУ так, чтобы часть сведений оказалась скрыта (например, изменить размеры ячейки в Excel). При работе по 44-ФЗ такое невозможно, потому что там все сведения подаются через стандартизированные формы. А вот для закупок по 223-ФЗ пока такая манипуляция не исключена.

Разновидностью манипуляций с требованиями к товарам является включение в описание таких недопустимых ограничений, как: требование, чтобы поставщик находился не более чем в 5 км от заказчика, наличие статуса официального дилера, наличие собственного офиса или требования к производственным мощностям. Установление подобных требований допускается в редких случаях и должно быть обосновано. При отсутствии таких обоснований подобные пункты рассматриваются как ограничения конкуренции и их можно и нужно обжаловать в ФАС.

На сайте государственных закупок <http://www.zakupki.gov.ru> мошенники используют несколько иную схему, которая также легко выявляется при тщательном изучении результатов торгов.

Государственная компания объявляет аукцион, на который выходят 3 организации. У 2-х из них явно не соответствует 2-я часть заявки, и они это знают. У 3-й все хорошо. После начала торгов 2 организации с фиктивными заявками начинают активно торговаться с максимальным шагом. Они опускают цену до порога рентабельности и ждут окончания аукциона. На этапе закрытия торгов 3-я организация подает предложение максимально близкое к стартовой (чтобы оказаться на 3-м месте). В такой ситуации остальные участники аукциона не имеют возможности нормально торговаться, т. к. придется соревноваться с организациями, которым победа не грозит, и они демпингуют цены, или угадывать на последних секундах ставку 3-й организации.

Выявление указанных схем возможно путем анализа из открытых источников: аффилированности организаций, оборота их финансовой

деятельности, персональных данных учредителей, количеством выигранных тендеров и т.д.

Контрольные вопросы

1. Какую роль играют правила формирования запросов в поисковых системах Интернет?
2. Назовите известные Вам правила построения поисковых запросов.
3. Какие виды информации и по каким характеристикам возможно искать используя поисковые системы общего пользования и специализированные поисковые ресурсы?
4. Что такое метаданные файла? Какую информацию можно получить при изучении метаданных файлов фотоснимков?
5. Какие Вам известны средства и методы поиска криминалистически значимой информации в мессенджерах?
6. Какие методы OSINT позволяют обнаружить удаленные страницы или удаленные данные на страницах интернет-сайтов?
7. Сформулируйте понятие парсинга. Приведите примеры методов и средств парсинга.
8. Сформулируйте понятие больших массивов данных (*Big Data*). Назовите возможные направления использования результатов обработки «больших данных» в расследовании преступлений.
9. Назовите задачи расследования, которые можно решать с использованием нейросетей общего доступа.
10. Назовите известные Вам направления использования результатов поиска и анализа информации в открытых сетевых базах данных.

3. УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ И ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ФИКСАЦИИ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, ОБНАРУЖЕННОЙ НА РЕСУРСАХ СЕТИ ИНТЕРНЕТ

Использование результатов поиска и анализа информации на ресурсах сети Интернет в досудебном производстве сталкивается с рядом проблем. На это обратил внимание Бахтеев Д. В. Согласившись с мнением Янгаевой М. О. и Павленко Н. О., он указал что, учитывая пассивный характер сведений, собираемых с помощью OSINT, они могут являться лишь ориентирующими, но не доказательственными, поскольку отсутствует прямая доказательственная связь между человеком (организацией) и полученными сведениями. Учитывая востребованность OSINT-методов в разных отраслях человеческой деятельности и большую конкуренцию на рынке разработчиков этих методов, их следует считать достаточно точными, однако OSINT может быть использован исключительно для «выдвижения версий, определения направлений расследования, планирования следственного действия, прогнозирования возможной линии поведения участников уголовного процесса и возможного противодействия расследованию», но не для, например, предъявления обвинения¹.

Методы OSINT не относятся к числу технических и тактических приемов производства следственных и иных процессуальных действий, направленных на собирание доказательств, поэтому сведения, полученные при их применении, не могут напрямую использоваться в доказывании. Однако результаты OSINT и анализа данных представляют ценность как любая иная информация об обстоятельствах, подлежащих установлению и доказыванию по уголовному делу.

На основании полученных сведений следователь выдвигает версии об источниках доказательственной информации, ее характере; определяет процессуальные средства собирания; планирует тактику их производства.

Важнейшим условием получения доказательств с ресурсов сети Интернет является соблюдение процессуальной формы деятельности, реализация технических и тактических рекомендаций по фиксации информации в электронно-цифровой форме.

Представляется необходимым в текущей работе представить ряд таких рекомендаций правового и тактического характера, применение которых, по мнению авторов, послужит формированию доказательств на основе данных, полученных в рамках поисковой деятельности следователя в сетевой среде.

При совершении мошенничества и других сетевых преступлений организованными группами, имеющими международный состав, выход за пределы национальных границ и использование ими возможностей глобальной информационной сети Интернет обусловлены прежде всего взаимосвязанным процессом экономической и криминальной глобализации.

Международные компьютерные сети позволяют осуществлять деятельность на такой территории, где может действовать (намеренно или

¹ Бахтеев, Д. В. Проблемы OSINT как источника криминалистически значимых сведений // Цифровые технологии и право : сборник научных трудов II Международной научно-практической конференции : в 6 т., Казань, 22 сентября 2023 года. – Казань: Познание, 2023. С. 36-39.; Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет//Алтайский юридический вестник. 2022. №2 (38). С. 131-135.

непреднамеренно) принцип экстерриториальности. Правоохранительные органы могут в данном случае осуществлять обмен информацией, хотя расцениваться с правовой точки зрения эта информация может по-разному, в зависимости от особенностей национального законодательства.

В соответствии с п. 1 ст. 2 УПК РФ производство по уголовному делу на территории Российской Федерации независимо от места совершения преступления ведется в соответствии с нормами соответствующего Кодекса, если международным договором Российской Федерации не установлено иное¹. В результате производства следственных действий могут возникать случаи, когда размещенные на ресурсах сети сведения, которые физически находятся на территории других государств, считываются, копируются или, возможно, уничтожаются. С точки зрения государства, в котором велся поиск данных, такие действия могут образовывать состав уголовного преступления в соответствии с внутренним уголовным правом, а также являться нарушением национального суверенитета.

В соответствии со ст. 7 Федерального закона «Об информации, информационных технологиях и о защите информации», к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Имеющиеся в любых разделах сети данные можно рассматривать как общедоступные, если доступ к ним не ограничен, и по этой причине вопрос о порядке их собирания и использования в качестве доказательств по уголовным делам регулируется исключительно внутренним, а не международным правом. Международные нормативные правовые акты также не запрещают подобное вмешательство, поскольку, с технической точки зрения, такие данные доступны и могут быть получены из государства, осуществляющего их поиск, без какой-либо помощи или вмешательства со стороны государства, где производится поиск таких данных. С учетом этого обращение к государству, где осуществляется поиск данных, не является необходимым ни на одном из этапов деятельности.

Важным условием в выборе способа и тактики фиксации доказательственной информации является обеспечение своевременного закрепления доказательств в электронном виде, отличающихся значительной динамичностью, особенно в условиях противодействия со стороны заинтересованных лиц. Оценка результата возможного противодействия расследованию преступлений имеет большое значение для планирования и организации работы следователя. При оказании такого противодействия в сфере компьютерной информации каждый очередной удачный факт сокрытия преступления позволяет правонарушителю осознать, насколько примененные им методы были адекватны поставленной задаче, и на основании этого решить вопрос о возможности применения новых. Кроме того, каждый случай подобного рода действий – это возможность для преступника еще лучше освоиться в виртуальной среде компьютерной информации. При этом он оценивает то, какие средства являются наиболее эффективными для достижения поставленных им преступных целей, при необходимости эти средства тиражирует и совершенствует.

¹ Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 31.12.2017) // Собр. законодательства Рос. Федерации. 1996. № 25. Ст. 2954.

Использование конкретных способов и средств фиксации информации, хранящейся на ресурсах сети Интернет, должно обеспечивать получение сведений, обладающих свойствами доказательств.

Для этого необходимо сочетание технических методов, делающих невозможным сам факт внесения изменений, и тактических, использующих процессуальные возможности обеспечения достоверности и допустимости доказательств.

К тактическим приемам можно отнести использование определенных форм процессуального обеспечения подлинности результатов, например, производство действий при понятых, упаковку носителей информации, исключаящую её вскрытие без нарушения целостности и обеспечивающую невозможность иного внепроцессуального воздействия на саму информацию, записанную на носитель, и др.

Следователь при производстве осмотра места происшествия, осмотра предметов и документов, обыска и выемки, проверки показаний на месте (ст. ст. 176, 177, 182, 183, 194 УПК РФ) может применять несколько различных способов фиксации доказательственной информации в электронном виде. Обязательным способом выступает протоколирование следственного действия. Вспомогательными способами выступают изъятие электронного носителя информации и копирование криминалистически значимой информации на иной носитель. Средства фото- и видеосъемки используются для фиксации хода следственного действия, а при условии демонстрации данных на мониторе компьютера – и для их фиксации.

Электронный носитель, который используется для копирования, сам по себе не имеет никакого отношения к событию преступления, не связан с ним, выбор его зависит от материально-технической базы следствия и эффективности применения ее в конкретной ситуации.

Зафиксированные таким образом сведения относятся к категории вещественных доказательств (ст. 81 УПК РФ), так как они обладают признаками, присущими исключительно вещественным доказательствам:

- данные, имеющие отношение к делу, содержатся на них во внешних признаках (в зависимости от способа записи бинарного кода);

- могут служить средством для обнаружения преступления, установления фактических обстоятельств дела, выявления виновных либо опровержения обвинения или смягчения ответственности;

- в них реализован материальный способ получения, сохранения и передачи невербальной информации, имеющей отношение к делу.

При копировании данных с целью фиксации доказательственной информации в электронном виде возникают так называемые производные вещественные доказательства. Несмотря на то, что новый носитель информации отличается от первоначального тем, что может быть изготовлен из других материалов, иметь другой вес, цвет, форму, размер и т. п., использование специальных средств и методов, применяющихся при копировании, позволяет достаточно точно передать характер тех признаков в зафиксированных данных, которые имеют доказательственное значение. Кроме уже указанных выше причин использования электронных носителей информации в качестве производных вещественных доказательств, может возникнуть необходимость использовать их в качестве первоначальных, если в процессе производства будут установлены умышленные действия,

направленные на уничтожение носителя или самих данных, а также в случае их модификации.

Еще одним важным условием эффективной фиксации для целей доказывания информации, хранящейся на ресурсах сети Интернет, является наличие у следователя необходимого объема знаний и навыков работы с «электронными доказательствами».

Обнаружение и изучение криминалистически значимой информации на сетевых ресурсах путем применения методов OSINT позволяет следователю оценить возможность использования сведений в качестве ориентирующей информации или доказательства по уголовному делу. Например, в качестве ориентирующей информации могут выступать обнаруженные сведения о связях лиц в социальной сети, номера телефонов и другие данные. Доказательственное значение могут иметь размещенные мультимедийные материалы, переписка пользователей, данные геолокации и иные сведения об обстоятельствах, подлежащих доказыванию.

Перспектива использования обнаруженной информации в расследовании предопределяет необходимость ее процессуальной фиксации. Особую роль при производстве следственных действий в отношении сведений в электронно-цифровой форме составляет участие специалиста, что должно быть обязательно отражено в протоколе следственного действия. Процесс применения программ и полученные результаты протоколируются. Полученные сведения, имеющие ориентирующее и доказательственное значение, могут быть записаны на электронный носитель информации, распечатаны и оформлены в качестве приложения к протоколу следственного действия.

При работе с информацией необходимо помнить:

- информация, расположенная на сайтах, не статична, она постоянно изменяется, поэтому при фиксации такой информации обязательно отмечается время работы и часовой пояс;

- ссылки на ресурсы, содержащие автоматический переход, с технической точки зрения аналогичны самому ресурсу (на ресурсах социальных сетей расположены, например, ссылки на видео экстремистской направленности, а не само видео);

- для гарантированного поиска информации, содержащейся в федеральном списке экстремистских материалов, целесообразно использовать базы значений хеш-функций этой информации;

- при определении данных об источниках, которые участвуют в распространении информации, устанавливаются учётные данные программно-аппаратной части, а не личность пользователя;

- при копировании информации с серверов передачи и хранения данных фиксируется только необходимая информация, дисковый массив не изымается.

При подготовке к производству процессуальных действий специалист в качестве консультанта может оказать помощь следователю в разъяснении технических вопросов организации распространения информации в сети, особенностей используемого программного обеспечения, способов подключения к интересующим ресурсам, указать вероятные места обнаружения дополнительных виртуальных следов. С учетом полученных от специалиста сведений следователь планирует расследование, принимает решение о производстве необходимых следственных действий и выносит письменные поручения о проведении оперативно-розыскных мероприятий.

При работе с информацией, расположенной на открытых сетевых ресурсах, интернет-специалистов привлекают для выявления интересующей информации, определения данных об источниках, которые участвуют в распространении информации, и фиксации выявленной информации; в качестве консультанта.

Анкетирование следователей, расследующих дела о дорожно-транспортных преступлениях, показало, что ресурсы сети Интернет при производстве по делу используются преимущественно для размещения объявлений о поиске очевидцев происшествия, розыске скрывшихся с места происшествия транспортных средств или водителей. Данные объявления размещаются на сайтах органов внутренних дел либо в электронных версиях региональных СМИ.

Однако это лишь одно направление использования информационных ресурсов сети Интернет. Широкое распространение автомобильных видеорегистраторов повлекло появление в сети Интернет огромного количества видеозаписей дорожно-транспортных происшествий, выкладываемых в сеть очевидцами происшествия либо его участниками. Накоплению видеозаписей дорожно-транспортных происшествий способствует большое количество камер видеонаблюдения и видеомониторинга. Видеоролики часто выкладываются в социальных сетях, а также на соответствующих тематических сайтах и форумах.

Сама видеозапись, содержащаяся на каком-либо сайте, может служить самостоятельным доказательством при условии ее процессуальной фиксации путем изъятия электронного носителя информации или ее копирования. Приобщению в качестве вещественного доказательства соответствующего носителя должна также предшествовать проверка сведений, запечатленных в записи. Наибольшее познавательное значение в этом случае имеет производство видеотехнической, фоноскопической и портретной экспертиз для установления подлинности записи, времени и места съемки, идентификации запечатленных лиц и разрешения иных вопросов. Для установления источника происхождения видеозаписи желательно установить субъекта, ее разместившего.

Чтобы установить пользователя той или иной страницы социальной сети или разместившего интересующий нас контент, необходимо обладать информацией о его IP-адресе. Искомая информация может быть предоставлена непосредственно владельцами того интернет-ресурса, которым разыскиваемый абонент пользуется.

Знание IP-адреса пользователя позволяет установить провайдера, услугами которого он пользовался. В свою очередь провайдер уже имеет данные о фактическом местоположении точки доступа к проводному Интернету или о лице, которое приобрело SIM-карту.

Для получения сведений об IP-адресе следователю в соответствии с ч. 4 ст. 21 УПК РФ необходимо направить запрос руководству компании – владельцу социальной сети с просьбой предоставить сведения об IP-адресах, с которых происходил доступ к странице и ее регистрация, а также, соответственно, точные временные интервалы работы с этой страницей.

Для установления провайдера, предоставившего пользователю возможность выхода в Интернет, необходимо использовать базу данных

IP-адресов интернет-провайдеров, размещенную в открытом доступе на интернет-ресурсе <http://www.2ip.ru>.

После установления провайдера ему необходимо направить запрос о предоставлении регистрационных данных пользователя, которому в конкретное время присваивался конкретный IP-адрес. В запросе рекомендуется также предоставлять информацию и о посещаемых искомым субъектом в указываемое время интернет-ресурсах. Это позволит индивидуализировать пользователя в случае предоставления интернет-провайдером услуг связи нескольким пользователям через единый узел связи под идентичным IP-адресом (преимущественно встречается при предоставлении услуг GPRS-связи сотовыми компаниями).

Важным источником доказательственной и ориентирующей информации может являться содержание электронной переписки фигурантов дела, ведущейся с использованием различных почтовых интернет-сервисов.

Владелец почтового аккаунта может вести активную переписку с иными участниками дела, передавать разного рода и степени важности документы, отправлять аудио- и видеофайлы переговоров, а также файлы, несущие разного рода смысловую нагрузку.

Существенным недостатком электронной почты с позиции правоохранительной деятельности является то, что при прохождении регистрации для получения почтового ящика пользователь, вводя свои персональные данные (идентификационные данные), может ввести любые сведения, даже не принадлежащие ему. Это в значительной степени затрудняет действия по установлению принадлежности конкретного почтового ящика тому или иному реальному субъекту.

Для получения доступа к электронной почтовой переписке следователь с согласия руководителя следственного органа возбуждает ходатайство перед судом о производстве осмотра и выемки электронных сообщений или иных передаваемых по сетям электросвязи сообщений в соответствии со ст. 38, ч. 1 ст. 165, и ч. 7 ст. 185 УПК РФ.

В результате проведения выемки данной электронной информации следователем будут получены:

- регистрационные данные абонента почтового ресурса;
- электронный носитель с базой данных почтового ресурса, на котором происходила выемка электронной почтовой корреспонденции.

Полученные данные, изъятые следователем в ходе выемки на почтовом ресурсе, осматриваются в целях обнаружения следов преступления и выяснения обстоятельств, имеющих значение для раскрытия и расследования преступления.

Фактически только копирование как способ фиксации доказательственной информации может быть применено в отношении данных, хранящихся в облаке или на серверах компаний, представляющих услуги хранения и размещения медиаконтента (RUTUBE, ВКонтакте и т. п.)

Процедура копирования информации в процессе следственного действия должна позволять решать задачи обеспечения достоверности сведений и их неизменности в процессе хранения. Фиксация источника копирования информации должна обязательно осуществляться в протоколе следственного действия, в рамках которого это осуществляется.

Для того чтобы размещенные в сети Интернет видеоролики, тексты или аудиозаписи стали доказательством, необходимо их зафиксировать с учетом рекомендаций криминалистической тактики.

Если интересное видео размещено на страничке пользователя социальной сети или каком-либо сайте, то необходимо осмотреть данный сайт или страничку. Осмотр может быть проведен в кабинете следователя с использованием его рабочего компьютера. В протоколе осмотра описывается внешний вид сайта и все действия, выполняемые следователем при переходе по ссылкам и пунктам меню. Необходимо учитывать время осмотра (т. к. информация на сайте динамическая и может постоянно изменяться), т. е. каждое действие по фиксации информации обязательно должно иметь привязку ко времени. Нужно зафиксировать и указать в протоколе часовой пояс или время – UTC-Всемирное координированное время (англ. Coordinated Universal Time, фр. Temps Universel Coordonné). Указывается адрес каждого окна сайта (берется из заголовка строки браузера). Страницы сайта копируются с помощью штатных средств интернет-браузеров (меню «Сохранить страницу как») или используют специализированное программное обеспечение для копирования всего содержимого сайта.

В ряде случаев достаточно сделать скриншот страницы.

В протоколе обязательно необходимо указать технические средства (компьютер) и программное обеспечение, которые применялись при осмотре и копировании файлов. Скопированные файлы записываются на неперезаписываемый носитель и оформляются в качестве приложения к протоколу осмотра. Следует помнить, что на страницах социальных сетей и сайтах видеоролики обычно не хранятся. На них размещаются только ссылки для просмотра или скачивания. Сами ролики хранятся на серверах компаний, предоставляющих соответствующие услуги. Однако в правовом понимании размещение ссылок на ресурсе конкретного пользователя необходимо рассматривать как размещение соответствующих файлов, т. к. их активация приводит к получению необходимой информации.

Файлы, хранящиеся в облачных хранилищах, могут быть осмотрены и скопированы при наличии доступа к данным ресурсам. Для этого, как правило, необходимо установить сетевой адрес хранилища и данные для аутентификации. Сама процедура осмотра и копирования содержащихся там файлов осуществляется с учетом вышеуказанных рекомендаций для сайтов сети Интернет.

Гарантом достоверности происхождения скопированной информации является участие при производстве следственного действия понятых. При этом важно, чтобы они понимали суть производимых действий, т.е. на языке современного обывателя, были «продвинутыми пользователями» компьютерной техники. Использование технических средств фиксации хода и результата следственного действия взамен понятых возможно в случаях, предусмотренных ст. 170 УПК РФ, но использование видеозаписи в этом случае менее эффективно, чем участие понятых. Применение специальных технических средств и программного обеспечения для копирования информации является обязательным. В настоящее время технико-криминалистическое обеспечение правоохранительных органов средствами копирования информации в электронном виде сконцентрировано на разработке и внедрении аппаратно-программных комплексов, использующихся для

извлечения данных с электронных носителей информации. Среди них необходимо выделить дубликаторы, применяемые для копирования компьютерных носителей информации, имеющие возможность подключения через распространенные в настоящее время интерфейсы, НЖМД и различных флэш-носителей, а также средства для клонирования памяти мобильных средств сотовой связи и других носимых гаджетов. Использование специальных программ и аппаратно-программных комплексов значительно упрощает работу следователя, так как в них автоматизированы наиболее типичные действия при производстве следственных действий в отношении данных в электронном виде и реализованы функции решения задач обеспечения достоверности полученных копий.

Решение вопроса о комплексном программно-техническом обеспечении копирования данных с удаленных ресурсов решается не так эффективно. Однако в большинстве случаев необходимости копирования электронной информации это можно осуществить путем использования распространенного компьютерного оборудования и программных средств. Производство осмотра места происшествия либо предметов и документов, связанного с копированием данных с удаленных источников, целесообразно осуществлять с участием специалиста, однако реализация криминалистических рекомендаций позволяет осуществить его самостоятельно лицом, производящим следственное действие и имеющим навыки собирания «электронных доказательств».

Как было частично сказано выше, для копирования данных с удаленных источников следователю необходимо иметь компьютер, подключенный к сети Интернет, с приводом для записи CD-DVD дисков в том случае, если осмотр сайта или иного ресурса в сети происходит с рабочего места следователя. Когда же осмотр удаленного ресурса осуществляется в рамках рабочего этапа осмотра места происшествия (например, в ситуации, если в рамках осмотра на рабочем месте подозреваемого обнаруживается открытая сессия обмена данными с удаленным закрытым (облачным) хранилищем), бывает достаточно одного внешнего привода, подключаемого через USB-интерфейс. Также необходимо достаточное количество оптических дисков или иных электронных носителей информации, на которые предполагается копирование. Необходимое программное обеспечение включает в себя носители с portable-версиями программ, использующихся для копирования сайтов, скачивания файлов со специализированных ресурсов, на которых они выложены только для просмотра, для создания скриншотов или записи в видеофайл событий, демонстрируемых на мониторе компьютера, создания архивов скопированной совокупности файлов и подсчета хеш-сумм копируемой информации. Предназначение большинства перечисленных объектов для современных пользователей компьютерной техники не требует разъяснения.

Все из перечисленных программ представлены в интернете для свободного скачивания и использования различными разработчиками. Программы для копирования сайтов предназначены прежде всего для обеспечения возможностей пользователей знакомиться с содержимым сайта в автономном режиме (без подключения к интернету) после его скачивания на электронный носитель компьютера или съемный носитель. В отличие от использования функции браузеров «Сохранить как» использование таких программ позволяет сохранить структуру сайта с возможностью функционирования внутренних гиперссылок. Использование таких программ

удобно для оперативного копирования фишинговых сайтов: их внешнего вида, внутренней структуры и контента.

Программы для скачивания медиафайлов, размещенных для просмотра, обеспечивают их копирование даже в случае отсутствия такой возможности с помощью браузера. Эти программы могут быть в виде плагинов к браузерам или как отдельные программные продукты. Их использование уместно прежде всего для копирования различных видеороликов с записями преступных действий, которые выкладывают очевидцы на сайты (видеохостинги).

Возможность снятия скриншотов обеспечивает запись файлов с изображениями на мониторе компьютера в определенные моменты времени. Данная функция может быть реализована средствами операционной системы.

Клавиша на компьютерных клавиатурах PrtScr или Print Scrn обычно расположена в секции с клавишами Break и Scroll Lock. Print Screen находится на одной кнопке с SysRq. При ее нажатии в Windows изображение монитора копируется в буфер обмена и требует дальнейшего сохранения путем использования программ графических редакторов. Более удобны в использовании специальные программы для снятия скриншотов. При их применении обычно можно настроить параметры автоматического снятия скриншотов через определенные промежутки времени, выбрать формат файлов и адрес для их сохранения. Более широкие возможности для фиксации хода и результатов следственного действия представляют программы, осуществляющие запись изображения монитора в видеофайлы. Их использованием можно заменить обычную видеосъемку следственного действия в части осмотра содержимого удаленного ресурса.

Программы для определения хеш-суммы копируемой информации используются для её аутентификации, т. е. установления и подтверждения неизменности информации. Данный термин в области информационных технологий применяется для обозначения процедур проверки подлинности пользователя путём сравнения введённого им пароля с паролем в базе данных пользователей, подтверждения подлинности электронного письма путём проверки цифровой подписи по ключу проверки подписи отправителя; проверки контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

Чтобы предотвратить сомнения в том, что в процессе копирования информации или при ее хранении могли быть внесены изменения, необходимо вычислить контрольную сумму или хеш-сумму (данные термины являются синонимами) копируемых файлов или копируемых разделов электронного носителя информации до их копирования и после. Контрольные суммы необходимо переписать в протокол следственного действия.

Существует множество алгоритмов хеширования с различными свойствами (разрядность, вычислительная сложность, криптостойкость и т. п.). Выбор той или иной хеш-функции определяется спецификой решаемой задачи. Простейшими примерами хеш-функций могут служить контрольная сумма или CRC. При выборе программ для вычисления хеш-суммы копируемой информации необходимо учитывать, что «хорошая» хеш-функция должна удовлетворять двум свойствам: быстро вычисляться и минимизировать количество коллизий. Для решения обозначенных задач целесообразно применять программы, реализующие криптографические хеш-функции, т. е. стойкие к коллизиям, применяемые в криптографии.

Если лицо, производящее следственное действие, имеет электронную подпись, т. е. соответствующий набор программ, то для определения хеш-суммы копируемых данных целесообразно использовать сертифицированную программу, входящую в данный набор. Возможно использование и иных программ хеширования. Свободно распространяемыми программами, реализующими алгоритм хеширования, – MD5, являются md5summer и HashTab. Определение хеша по данному алгоритму реализовано и в достаточно популярной у пользователей файловой оболочке Total Commander.

Хеширование скопированных файлов и фиксация кода в протокол следственного действия обеспечивает возможность проверки их подлинности в любой момент времени. Вычисление хеша файлов, скопированных с пиринговых файлообменных сетей или ftp-серверов, позволяет также установить их аутентичность файлам, размещенным на соответствующих ресурсах, если лицо, их разместившее, указало значение функции в описании файлов.

Запись скопированных файлов рекомендуется осуществлять только на непереписываемый носитель, который будет прилагаться к протоколу следственного действия без создания мультисессии. Чтобы снизить риск случайного или умышленного изменения файлов в процессе их хранения или работы с ними, уместно записать их единым файлом архива, предварительно установив хеш каждого файла и хеш архива. Данные внести в протокол следственного действия.

Использование свободных программных продуктов, не сертифицированных ФСТЭК России, не противоречит нормам УПК РФ. Возникновение возможных сомнений в том, что такая программа может скрытно для пользователя реализовать вредоносные функции, в том числе изменить копируемые данные, устраняется путем приложения к протоколу следственного действия непереписываемого оптического диска или иного носителя, на которых записаны portable-версии использованных свободных программ, с которых они запускались. Если в процессе дальнейшего производства по делу будет установлено противоречие доказательств, его всегда можно будет устранить путем экспертизы вызвавших сомнение программ.

Контрольные вопросы

1. Обоснуйте позицию и выскажите мнение о возможности использования в доказывании сведений, полученных следователем в результате применения методов OSINT.

2. Сформулируйте понятие общедоступной информации. Обоснуйте возможность производства процессуальных действий в отношении сведений общедоступного характера, распространяемых в сети Интернет, но физически хранящихся на серверах на территории других государств.

3. Назовите процессуальные способы фиксации информации в электронно-цифровой форме.

4. Назовите тактические рекомендации по фиксации уголовно-релевантных видеофайлов, распространяемых на ресурсах видеохостингов.

5. Опишите тактический алгоритм установления лица, администрирующего пользовательский аккаунт сервиса социальной сети.

6. Опишите тактический алгоритм (алгоритмы) фиксации уголовно-релевантной информации, хранящейся в облачном хранилище.
7. Перечислите тактические рекомендации по копированию данных с удаленных ресурсов в рамках производства следственных действий.
8. Назовите способы проверки аутентичности данных в электронно-цифровой форме, зафиксированных при производстве следственных действий.

ЗАКЛЮЧЕНИЕ

В представленном пособии изложены учебные материалы и практические рекомендации по использованию субъектами расследования программных способов анализа больших объемов данных, а также поиска и аналитической обработки информации из открытых источников сети Интернет для формирования доказательств в досудебном производстве. Современные возможности информационных технологий и программных решений предопределяют необходимость их использования в процессе раскрытия и расследования преступлений, а также в формировании доказательственной базы в ходе досудебного производства по уголовным делам.

Изучение современных достижений в области информационных технологий в контексте возможности их использования при расследовании преступлений, программных методов поиска информации в сети Интернет, программных способов анализа больших объемов данных позволило предложить алгоритм действий по поиску и анализу информации из открытых источников в сети Интернет в зависимости от следственной ситуации, алгоритм использования полученной информации при проведении процессуальных действий и принятии процессуальных решений, а также сформировать рекомендации, направленные на признание результатов поиска и анализа информации в сети Интернет в качестве доказательств в ходе досудебного производства по уголовному делу.

Предложенные в конце каждого раздела вопросы для самоконтроля позволяют обучающимся выстроить траекторию последовательного изучения учебного материала, выделить наиболее значимые рекомендации по работе с данными в электронно-цифровой форме, проверить уровень и качество усвоения знаний.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). – Российская газета - 4 июля. [Электронный ресурс] // СПС «КонсультантПлюс». – URL: <http://www.consultant.ru> (дата обращения 26.06.2025).
2. Конвенция о защите прав человека и основных свобод (ратифицирована 4 ноября 1950 г. в г. Риме) [Электронный ресурс] // Сайт Совета Европы. – URL: <https://www.coe.int/ru/web/compass/the-european-convention-on-human-rights-and-its-protocols> (дата обращения: 26.06.2025).
3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 31.07.2025) // Собр. законодательства Рос. Федерации. – 1996. – № 25. – Ст. 2954.
4. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 31.07.2025) // Собрание законодательства РФ. – 2001. – № 52 (ч. I). – Ст. 4921.
5. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». – URL: <http://www.consultant.ru> (дата обращения 26.06.2025).
6. О полиции : Федеральный закон от 07.02.2011 № 3-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». – URL: <http://www.consultant.ru> (дата обращения 26.06.2025).
7. Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 г. № 144-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». – URL: <http://www.consultant.ru> (дата обращения 26.06.2025).
8. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления : Федеральный закон от 09.02.2009 № 8-ФЗ // СПС «КонсультантПлюс».
9. О включении сведений о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных» (Приложение № 1) : приказ Минкомсвязи России от 07.04.2020 № 162. – URL: <https://clck.ru/35xsDo> (дата обращения: 26.06.2025). Реестр программного обеспечения. – URL: <https://reestr.digital.gov.ru/reestr/307657> (дата обращения: 26.06.2025).
10. О Перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети Интернет в форме открытых данных : распоряжение Правительства РФ от 10.07.2013 № 1187-р // СПС «КонсультантПлюс».

11. О развитии искусственного интеллекта в Российской Федерации : указ Президента РФ от 10 октября 2019 г. № 490, которым была утверждена Национальная Стратегия развития искусственного интеллекта на период до 2030 г. [Электронный ресурс] // СПС «КонсультантПлюс». – URL: <http://www.consultant.ru> (дата обращения : 26.06.2025).

12. ГОСТ Р 59926-2021/ISO/IEC TR 20547 2:2018. Национальный стандарт Российской Федерации. Информационные технологии. Эталонная архитектура больших данных. Часть 2. Варианты использования и производные требования (утв. и введен в действие Приказом Росстандарта от 2 декабря 2021 г. № 1685-ст) // Москва : ФГБУ «РСТ», 2022. – URL: <https://clck.ru/35xtY4> (дата обращения: 26.06.2025).

Научная литература

1. Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис... канд. юрид. наук / А. А. Балашова. - Москва, 2020. - 216 с.

2. Бахтеев Д. В. Проблемы OSINT как источника криминалистически значимых сведений // Цифровые технологии и право : сборник научных трудов II Международной научно-практической конференции : в 6 т., Казань, 22 сентября 2023 года. – Казань : Познание, 2023. – С. 36-39.

3. Ваценко А. А. Обзор техник компьютерной криминалистики / А. А. Ваценко // Бюллетень науки и практики. - 2020. - № 6. - С. 164-170.

4. Вехов В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства / В. Б. Вехов // Российский следователь. - 2013. - № 10. - С. 22–24.

5. Вехов, В. Б. Электронные следы в системе криминалистики / В. Б. Вехов, Б. П. Смагоринский, С. А. Ковалев // Судебная экспертиза. - 2016. - № 2 (46). - С. 10–19.

6. Григорьев О. Г. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства: автореф. дис....канд. юрид. наук / О.Г. Григорьев. – Омск, 2003. - 25 с.

7. Ищенко Е. П. Криминалистика : учебник / Е. П. Ищенко, А. А. Топорков, под ред. Е.П. Ищенко. 2-е изд., испр., доп. и перераб. Москва : КОНТРАКТ, ИНФРА-М, 2010. – 780 с.

8. Желева О. В. К вопросу о понятии электронных доказательств и критериях допустимости их использования / О. В. Желева // Уголовная юстиция. – 2021. – № 17. – С. 44-48.

9. Зазулин А. И. Osint для адвоката. Как работать и источниками информации в интернете / А.И. Зазулин // Уголовный процесс. – 2021. – № 10(202). – С. 90-96.

10. Зигура Н. А. Компьютерная информация как вид доказательств в уголовном процессе России : дис. ... канд. юрид. наук / Н. А. Зигура. – Челябинск, 2010. - 234 с.

11. Зуев С. В. О современной концепции развития информационных технологий в уголовном судопроизводстве (РИТВУС) / С. В. Зуев // Пермский юридический альманах. – 2019. – № 2. – С. 618–629.

12. Зуев С. В., Титова А. С. Слабые стороны информационного подхода в свете цифровизации уголовного судопроизводства / С. В. Зуев, А. С. Титова // Правопорядок: история, теория, практика. – 2019. – № 1. – С. 49-54.
13. Краснова Л. Б. Электронные носители информации как вещественные доказательства / Л. Б. Краснова // Известия Тульского государственного университета. Экономические и юридические науки. – 2013. - № 4-2. – С. 254–260.
14. Лазарева В. А. Доказывание в уголовном процессе / В. А. Лазарева. Москва, 2009. – 344 с.
15. Осипенко А. Л., Гайдин А. И. Правовое регулирование и тактические особенности изъятия электронных носителей информации / А. Л. Осипенко, А. И. Гайдин // Вестник Воронежского института МВД России. – 2014. – № 1. – С. 156-163.
16. Овсянников Д. В. Копирование электронной информации как средство уголовно-процессуального доказывания : автореф дис. ... канд. юрид. наук / Д. В. Овсянников. – Екатеринбург, 2015. – 21с.
17. Пастухов П. С., Терехин В. В. К вопросу о понятии и сущности электронных доказательств в уголовном процессе / П. С. Пастухов, В. В. Терехин // Вестник Коми Республиканской академии государственной службы и управления. Серия: Государство и право. – 2014. – № 18. – С. 69–75.
18. Салиев А. А. К понятию о роли специальных знаний используемых в ходе расследования преступлений / А. А. Салиев // European journal of law and political sciences. – 2016. – № 4. – С. 76-80.
19. Смушкин А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений / А. Б. Смушкин // Актуальные проблемы российского права. – 2022. – № 3. – С. 102-111.
20. Терехов А. М. Моделирования и прогнозирования преступности: теоретический аспект / А. М. Терехов // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2021. – № 2. – С. 120-127.
21. Титова К. А., Литвинова И. В. К вопросу о возможности применения существующих критериев допустимости доказательств к электронным доказательствам в Российском уголовном процессе / К. А. Титова, И. В. Литвинова // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. – 2022. – № 2(91). – С. 144-151.
22. Ткачев, А. В. Вопросы использования электронных носителей компьютерной информации в уголовном процессе в качестве доказательств иных документов / А. В. Ткачев // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – № 3-2. – С. 436–442.
23. Хамидуллин, Р. С. Криминалистическое обеспечение использования технологии искусственного интеллекта в раскрытии и расследовании преступлений / Р. С. Хамидуллин // Российский юридический журнал : электронное приложение. – 2024. – № 2. – С. 19–29. – DOI: 10.34076/221968382024_2_19.
24. Черданцев, А. Ю. Понятие цифровых доказательств, современное состояние и их роль в доказательственном процессе / А. Ю. Черданцев // Юридическая наука и практика. – 2019. – Т. 15, № 4. – С. 55–60.
25. Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет / М. О. Янгаева,

Н. О. Павленко //Алтайский юридический вестник. – 2022. – №2 (38). – С. 131-135.

26. Яковлева К. Ю. Использование технологии OSINT в ходе обыска места нахождения электронной информации / К. Ю. Яковлева // Проблемы правовой и технической защиты информации. – 2023. - №11. - С. 131-136.

Материалы судебной практики

1. Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Рос. Федерации от 13 декабря 2018 г. по делу № 4-АПУ18-41 [Электронный ресурс] // Legalacts.ru: законы, кодексы и нормативные правовые акты в Рос. Федерации. – URL: – <https://legalacts.ru/sud/apellia-tsionnoe-opredelenie-ver-khovnogo-suda-rf-ot-13122018-n-4-apul8-41/> (дата обращения: 09.06.2025).

2. Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Рос. Федерации от 10 декабря 2019 г. по делу № 223-АПУ19-1 [Электронный ресурс] // Судебные и нормативные акты Рос. Федерации. – URL: <https://sudact.ru/vsrf/-doc/pQ6xljelyiVL/> (дата обращения: 26.06.2025).

3. Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Рос. Федерации от 3 июля 2013 г. по делу № 46- АПУ13-10 // Сайт Верховного Суда Рос. Федерации. – URL: <https://vsrf.ru/lk/practice/cases/5567789#55677-89> (дата обращения: 26.06.2025).

4. Приговор Комсомольского районного суда г. Тольятти от 10 февраля 2020 г. по делу № 1-9/2020 (1- 408/2019) [Электронный ресурс] // Сайт Комсомольского районного суда г. Тольятти. – URL: https://kom-somolsky-sam.sudrf.m/modules.php?name=sud_delo&name_op=case&_id=162685477&_uid=6e33ecdb-4355-4475-8ac5-3c57de787e5-d&_deloId=1540006&_caseType=0&_new=0&srv_num=1 (дата обращения: 26.06.2025).

5. Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Рос. Федерации от 26 декабря 2012 г. по делу № 48-012-112 [Электронный ресурс] // Сайт Верховного Суда Рос. Федерации. – URL: <https://vsrf.ru/lk/practice/cases/5575441#5575441> (дата обращения: 26.06.2025).

6. Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Рос. Федерации от 5 июня 2020 г. по делу № 225-АПУ20-3 [Электронный ресурс] // Legalacts.ru: законы, кодексы и нормативные правовые акты в Рос. Федерации. – URL:<https://legalacts.ru/sud/apelliatsionnoe-opredelenie-sudebnoi-kollegii-po-delam-voennosluzhashchikh-verkhovnogo-suda-rossiiskoi-federatsii-ot-05062020-n-225-ari20-3/> (дата обращения: 26.06.2025).

7. Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Рос. Федерации от 1 августа 2019 г. по делу № 67-АПУ19-8 [Электронный ресурс] // Legalacts.ru: законы, кодексы и нормативные правовые акты в Рос. Федерации. – URL: <https://legalacts.ru/sud/apelliatsionnoe-opredelenie-sudebnoi-kollegii-po-ugolovnym-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-01082019-n-67-apul98/> (дата обращения: 26.06.2025).

Иные источники

1. Состояние преступности в России: статистические данные, – URL: <https://мвд.рф/reports> (дата обращения: 22.09.25).

2. Сколько пользователей интернета в мире? Статистика интернет – медиа. [Электронный ресурс], – URL: <https://inclient.ru/users-internet-stats/> (дата обращения 30.09.2025).

Учебное издание

Гайдин Александр Иванович
Смагин Павел Геннадьевич
Гущин Александр Николаевич
Савицкая Ирина Геннадьевна
Красноруцкая Татьяна Александровна
Тишкин Сергей Владимирович

**ФОРМИРОВАНИЕ ДОКАЗАТЕЛЬСТВ В ДОСУДЕБНОМ ПРОИЗВОДСТВЕ
НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ СЛЕДОВАТЕЛЕМ ПРОГРАММНЫХ
СПОСОБОВ АНАЛИЗА БОЛЬШИХ ОБЪЕМОВ ДАННЫХ, А ТАКЖЕ
ПОИСКА И АНАЛИТИЧЕСКОЙ ОБРАБОТКИ ИНФОРМАЦИИ
ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ СЕТИ ИНТЕРНЕТ**

Учебное пособие

Редактор В.Ю. Калининская
Компьютерная верстка А.И. Гайдина

Подписано в печать 30.03.2026

Формат 60x84^{1/16}

Усл. печ. л. 3,26

Тираж 90 экз. Заказ № 64

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394065, Воронеж, просп. Патриотов, 53