РЯСОВ АЛЕКСАНДР АЛЕКСЕЕВИЧ
кандидат юридических наук, доцент
Ставропольский филиал
Краснодарского университета МВД России (Ставрополь, Россия)
identifiks@mail.ru

БАГИРОВ ЗАУР РУСЛАНОВИЧ
Северо-Кавказский институт повышения квалификации (филиал)
Краснодарского университета МВД России (Нальчик, Россия)
bagirov07.05@gmail.com

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ СОЦИАЛЬНЫХ СЕТЕЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Аннотация: *В условиях современного информационного общества социальные сети занимают важное место в повседневной жизни миллионов людей. Эти платформы предоставляют широкие возможности для коммуникации, обмена информацией и самовыражения, однако одновременно создают новые вызовы для правоохранительных органов. Статья рассматривает вопросы использования социальных сетей в процессе расследования преступлений, акцентируя внимание на правовых аспектах и практических методах получения розыскной и доказательственной информации.*

Рассматривается широкий спектр инструментов, применяемых для извлечения данных из социальных сетей, начиная от официальных запросов к администраторам соцсетей и заканчивая осмотром и изъятием электронных устройств. Освещается процесс мониторинга активности пользователей, который позволяет выявлять потенциальные угрозы и собирать важные доказательства. Также уделяется внимание особенностям работы с открытыми источниками информации, такими как публичные посты, комментарии и фотоальбомы.

Особое внимание в статье уделяется проблемам, связанным с использованием социальных сетей в следственной практике. Приводятся практические рекомендации по эффективному применению социальных сетей в ходе расследования преступлений, а также рассматриваются перспективы дальнейшего развития данного направления.

Ключевые слова: *социальные сети, расследование преступлений, доказательственная информация, правовые аспекты, мониторинг активности, открытые источники, анонимность, персональные данные, доступ к аккаунтам, цифровые следы, методы анализа данных*

Для цитирования: *Рясов А.А., Багиров З.Р. Возможности использования социальных сетей при расследовании преступлений // Вестник ВИПК МВД России. 2025. № 1(73). С. 157-162; https://doi.org/:10.29039/2312-7937-2025-1-157-162.*

RYASOV ALEXANDER A.
PhD, associate professor
Stavropol branch of the Krasnodar University of the Ministry of Internal Affairs of Russia (Stavropol, Russia)
BAGIROV ZAUR R.
North Caucasian Institute for Advanced Studies (branch) Krasnodar University of the Ministry of Internal Affairs of Russia (Nalchik, Russia)

THE POSSIBILITIES OF USING SOCIAL MEDIA IN THE INVESTIGATION OF CRIMES

Abstract. *In the modern information society, social networks occupy an important place in the daily lives of millions of people. These platforms provide ample opportunities for communication, information exchange and self-expression, but at the same time create new challenges for law enforcement agencies. The article examines the use of social networks in the process of investigating crimes, focusing on the legal aspects and practical methods of obtaining investigative and evidentiary information.*

A wide range of tools used to extract data from social networks is considered, ranging from official requests to administrators of social networks and ending with the inspection and seizure of electronic devices. The process of monitoring user activity is highlighted, which makes it possible to identify potential threats and collect important evidence. Attention is also paid to the specifics of working with open sources of information, such as public posts, comments, and photo albums.

The article pays special attention to the problems related to the use of social networks in investigative practice. Practical recommendations on the effective use of social networks in the course of crime investigation are given, as well as prospects for further development of this area are considered.

Keywords: *social networks, crime investigation, evidentiary information, legal aspects, activity monitoring, open sources, anonymity, personal data, account access, digital traces, data analysis methods*

For citation: *Ryasov A.A., Bagirov Z.R. The possibilities of using social media in the investigation*
of crimes // Vestnik Advanced Training Institute of the MIA of Russia. 2025. № 1 (73). P. 157-162; https://doi.org/:10.29039/2312-7937-2025-1-157-162.

Вступительная часть.

Современный мир стремительно меняется под влиянием информационных технологий, и одним из самых заметных феноменов последних десятилетий стало появление и распространение социальных сетей. Сегодня эти платформы стали неотъемлемой частью повседневной жизни миллиардов людей по всему миру. Пользователи делятся своими мыслями, фотографиями, видео, общаются с друзьями и коллегами, участвуют в обсуждениях актуальных событий. Однако помимо очевидных преимуществ, социальные сети представляют собой новый вызов для правоохранительных органов, поскольку они могут содержать ценную информацию, которая способна существенно повлиять на ход расследования преступлений.

Несмотря на то, что использование социальных сетей в целях расследования преступлений представляет собой относительно новое направление, оно уже активно применяется в различных странах мира. Правоохранительные органы всё чаще обращаются к данным, размещённым в соцсетях, чтобы установить личность подозреваемых, выявить связи между участниками преступных группировок, найти свидетелей и собрать иные доказательства. Тем не менее этот процесс сопряжён с рядом юридических и технических сложностей, связанных с защитой персональных данных, обеспечением конфиденциальности и соблюдением прав граждан.

Целью настоящей статьи является исследование возможностей использования социальных сетей в процессе расследования преступлений. Мы рассмотрим правовые аспекты, методы получения доказательственной информации, особенности работы с электронными носителями и открытые источники данных. Особое внимание будет уделено вопросам достоверности информации, анонимности пользователей и сохранению доказательств. Кроме того, мы проанализируем существующие проблемы и предложим пути их решения, а также обсудим перспективы дальнейшего развития данного направления.

Основная часть.

Социальные сети глубоко проникли в повседневную жизнь современного человечества. Культурные ценности, включая развлекательные и рекреационные ресурсы, подвергаются цифровой трансформации. Около четырех миллиардов человек используют социальные сети каждый месяц, что подтверждается различными опросами. Согласно отчету Global Digital за 2024 год, число аккаунтов в социальных сетях возросло на 5,6% за последний год. Только за 2023 год к социальным сетям присоединилось 266 млн новых пользователей. Сегодня среднестатистический пользователь тратит на соцсети 2 часа

23 минуты ежедневно. В совокупности, человечество будет проводить в социальных сетях около 500 млн лет в 2024 году [1].

Несмотря на блокировку Facebook, Twitter и Instagram в России, многие пользователи всё ещё находят пути обхода этих ограничений с помощью VPN и прокси-серверов. Однако большинство российских пользователей предпочли переместиться на отечественные социальные сети.

Культурный контекст, государственная политика и языковые предпочтения оказывают существенное влияние на выбор социальных сетей по всему миру. В каждой стране пользователи предпочитают разные платформы. Например, в Китае широкое распространение получил WeChat, а в России огромную популярность завоевал, «ВКонтакте» и «Одноклассники». Некоторые страны создают собственные платформы, чтобы удовлетворить уникальные культурные и языковые запросы своих пользователей.

Социальные сети используются для общения, обмена информацией, создания контента и даже ведения бизнеса. Однако их потенциал выходит далеко за рамки обычного взаимодействия между пользователями. В последние годы социальные сети все чаще привлекают внимание правоохранительных органов как важный инструмент в процессе расследования преступлений.

Социальные сети таят в себе значительную угрозу — риск утечки личной информации. Нередко пользователи публикуют в своих профилях такие данные, как дата рождения, номер телефона, место работы, что дает злоумышленникам возможность сформировать детальный психологический портрет и получить доступ к другой ценной информации. Эти сведения могут использоваться мошенниками для обмана, выдавая себя за другого человека, нанесения ущерба профессиональной репутации и разрушения личных отношений.

Рост популярности социальных сетей также привёл к появлению новых возможностей для экстремистской деятельности, включающей распространение идей ненависти, вербовку и координацию действий. Пропаганда ксенофобии всё реже осуществляется через привычные методы, такие как демонстрации или печатная продукция, вместо них экстремисты предпочитают использовать разнообразные виды цифрового контента. Платформы типа Facebook, Twitter и Telegram становятся инструментами для преступников и радикалов, помогающими продвигать свои идеи и привлекать новых приверженцев.

Присоединение к некоторым группам в социальных сетях может привести к контакту с подпольным рынком запрещенных товаров и услуг. По мере роста числа киберпреступлений, зачастую приобретающих международный масштаб и представляющих серьёзную опасность, социальные сети выполняют двоякую функцию.

Одна из ключевых проблем связана с интерпретацией информации следователями. Несмотря на то, что криминалистическая наука подчеркивает значение индивидуального подхода к исследованию личности обвиняемого или подозреваемого, на практике этот принцип нередко остается нереализованным. Со временем, работая с подобными категориями преступников, следователи начинают формировать стереотипные представления о характерных чертах этих людей. Эти обобщения могут быть перенесены на конкретного обвиняемого, вытесняя собой слабо изученные или совсем неизвестные аспекты его личности. Это создает угрозу замены объективного знания субъективным мнением, что может привести к ошибочным заключениям и неправильным действиям следователя при оценке личности обвиняемого или подозреваемого. В итоге возрастает риск принятия неверных решений по делу.

Исходя из этого, использование социальных сетей в контексте криминалистического исследования личности обвиняемого или подозреваемого должно восприниматься как дополнительный инструмент. Анализ информации из соцсетей дает возможность быстро, хотя и неофициально, получить предварительную информацию о человеке, а также собрать дополнительные данные для более глубокого понимания его личности или обстоятельств дела. Однако, учитывая природу этого источника, его следует рассматривать только как дополнение, а в некоторых случаях его использование может быть невозможно или нежелательно.

Разведка на основе открытых данных (OSINT) подразумевает использование общедоступной информации, которая собирается из различных публичных ресурсов. В этой деятельности активно задействуются специализированные поисковые системы. Сфера применения OSINT включает анализ пользовательских профилей, отслеживание

их действий и связей в соцсетях, определение географического положения и многое другое. Существует множество бесплатных инструментов, таких как Яндекс и Google, которые используются для выполнения специфических запросов. Коммерческих решений тоже немало, хотя те, что используют искусственный интеллект, пока встречаются редко.

Для следователя наибольший интерес представляют не столько рутинные поиски информации в социальных сетях, проводимые вручную сотрудниками органа дознания, экспертами или специалистами, сколько использование специализированного программного обеспечения, предназначенного для анализа больших объемов данных. Эти технологии дают возможность правоохранительным структурам выявлять стабильные группировки и неявные связи между разными людьми, устанавливать взаимодействие между подозреваемыми, жертвами и иными участниками преступлений, предсказывать вероятность совершения определённых преступлений конкретной группой пользователей, искать свидетелей происшествий (например, тех, кто оставил сообщения или фотографии, подтверждающие их присутствие на месте события), а также получать данные о подготовке актов насилия.

В арсенале OSINT имеются различные сервисы и программы, среди которых выделяются такие, как Foca, Shodan, Email2phonenumber, Emailsherlock, Search4Faces и др.

FOCA [2] — это программа, специально разработанная для поиска метаданных и скрытой информации в документах, подлежащих сканированию. Эти документы могут располагаться на веб-сайтах и загружаются для анализа с помощью данного инструмента.

Программа способна работать с разнообразными форматами документов, наиболее распространёнными из которых являются файлы Microsoft Office, Open Office или PDF, но она также поддерживает работу с другими типами файлов.

Shodan [3] кардинально отличается от Google, который фокусируется на индексации сайтов и статей, предназначенных для широкого круга пользователей. Shodan занимается индексацией всех устройств, подключённых к интернету, будь то веб-камеры, маршрутизаторы или иные устройства, и предоставляет возможность находить их с помощью сложных поисковых запросов и фильтров.

При помощи инструментов сканирования серверов Shodan осуществляет проверку значительной доли адресного пространства IPv4. Главная задача — обнаружить каждое устройство, связанное с интернетом, и сохранить его уникальный «цифровой отпечаток». Сканеры Shodan определяют, какие сетевые функции выполняет каждое найденное устройство, а также собирают данные заголовков, позволяющие идентифицировать используемое ПО или аппаратное обеспечение. Все собранные данные сохраняются в базе данных Shodan, что позволяет пользователям выполнять поиск по конкретному программному обеспечению и находить устройства в интернете, на которых оно установлено.

Поиск документов осуществляется с использованием трёх поисковых систем: Google, Bing и DuckDuckGo. Совместные результаты всех трёх поисковиков предоставляют значительный объем документов. Дополнительно можно добавлять локальные файлы для извлечения метаданных из изображений.

Email2Phonenumber [4] — это инструмент, который позволяет узнать номер телефона пользователя, располагая его адресом электронной почты. Работает он на основе анализа уязвимостей в процессах восстановления паролей и использования данных, находящихся в открытом доступе. Таким образом, программа демонстрирует, как подобные уязвимости могут применяться для разведывательных целей. Она наглядно показывает, какие риски связаны с безопасностью множества онлайн-сервисов, и подчёркивает необходимость защиты личной информации пользователей.

Основные функции Email2Phonenumber заключаются в следующем:

сбор фрагментарных данных о номере телефона с сайтов, запускающих процедуру восстановления пароля, где требуется ввод электронного адреса. Инструмент проверяет, отображаются ли части номера телефона в ходе этого процесса;

формирование списка возможных телефонных номеров на основе масок, характерных для конкретной страны;

последовательная проверка сгенерированных номеров путём отправки запросов на восстановление пароля для нахождения совпадений с частично скрытым электронным адресом.

EmailSherlock [5] — это веб-ресурс, созданный для поиска адресов электронной почты. Запущенный в 2006 году, сайт изначально задумывался как помощник для пользователей, стремящихся найти электронную почту определенного человека или организации. Со временем сервис расширил свой функционал, добавив такие возможности, как обратный поиск по электронной почте, углубленный веб-поиск и поиск по доменам. На сегодняшний день EmailSherlock считается одной из самых востребованных и надёжных платформ для поиска электронных писем.

Search4faces [6] предназначен для пользователей социальных сетей. Этот сервис позволяет находить профили по аватаркам и другим изображениям. Поддерживаются такие платформы, как ВКонтакте, Одноклассники, TikTok и многие другие.

Это далеко не исчерпывающий список программ, помогающих поиску лица по открытым источникам.

Использование инструментов OSINT для мониторинга соцсетей открывает новые возможности для правоохранительных структур в расследовании правонарушений. Однако следует помнить о том, что для проведения подобных поисков следует использовать только пассивные поисковые средства, т.е. исключающие взаимодействие с удаленным устройством. Активный поиск может осуществляться только в рамках судебного решения. В противном случае ищущий сам может стать фигурантом уголовного дела.

Помимо этого, в процессе раскрытия и расследования преступлений могут быть задействованы такие возможности социальных сетей, как публикация правоохранительными органами сообщений, фотографий или описаний подозреваемых, а также обращения к обществу с просьбой сообщить о подозрительной активности или разыскиваемых преступниках.

Возможно также создание фейковых учетных записей сотрудниками правоохранительных служб для скрытого контроля над онлайн-сообществами и установления контактов с участниками закрытых групп, что также является значимым элементом работы по выявлению противоправных деяний.

Средствами пассивного поиска в OSINT может быть изучение метаданных файлов, поиск по изображениям, изучение данных, предназначенных для конфиденциального использования, но по ошибке выложенных в общую сеть, проверка адресов электронных почт, номеров телефонов и т.д.

Какую же информацию мы можем получить при производстве поисковых мероприятий из различных социальных сетей?

Изучая такие популярные в России социальные сети, как «ВКонтакте» и «Одноклассники» можно получить информацию о аватарках и типе профиля, статусах, лайках, репостах, комментариях, записях на стене, количестве друзей, его увлечениях (музыка, видео, фото), переписке, фотографиях человека, его связях, родственниках, местах проживания и местах времяпрепровождения, дате рождения, семейном положении, месте работы, времени создания профиля, адресе электронной почты, группах, в которых состоит человек, номере телефона, запланированных им событиях, праздниках, любимых играх, времени и месте учебы, уровне образования, финансовом положении, наличии домашних животных, подключенных платных функциях, совершенных им транзакциях и др.

Процесс сбора доказательств и ориентирующих данных, имеющих значение для следователей, предполагает проведение комплекса поисковых операций, выполняемых, как правило, сотрудниками органа дознания с помощью разнообразных методик.

Получение доступа к криминалистически значимой информации возможно с использованием компьютеров и мобильных устройств для доступа к страницам пользователей в социальных сетях, содержащих потенциально важную для расследования информацию, а также дальнейшее фиксирование этой информации путем фотографирования экрана монитора или создания скриншотов. Обнаружить такую информацию удается, когда интересующая следствие информация находится в свободном доступе или когда сотрудники органа дознания получают к ней доступ.

Возможно также и прямое подключение к электронным устройствам подозреваемого или пострадавшего, используя их аккаунты в социальных сетях. Это допускается либо с их согласия, либо на основании судебного решения.

Одним из дополнительных методов получения доказательственной информации в ходе расследования является получение данных с серверов компаний, предоставляющих услуги социальных сетей и/или мессенджеров, где хранится информация о пользователях. Это происходит путем отправки официальным запросам и получения соответствующих ответов, после чего эти данные присоединяют к материалам уголовного дела в виде иных документов.

В современных условиях социальные сети, с одной стороны, служат мощным инструментом коммуникации, позволяющим пользователям реализовывать своё право на свободу мысли и её выражения, а с другой стороны, они представляют собой публичную платформу, содержащую огромный объём данных, которые имеют высокую ценность для расследования киберпреступлений.

Практика показывает, что при расследовании подобных дел возникают сложные вопросы, касающиеся криминалистического сопровождения, внедрения инновационных технологий, участия экспертов, оптимизации процессов сбора, анализа и дальнейшего использования данной информации [7, с. 131-136]. Этот подход значительно повышает эффективность следственной и судебной практики и способствует её улучшению. Хотя использование информации из социальных сетей в уголовном процессе имеет свои плюсы, оно также связано с рядом трудностей и неопределённостей, требующих дополнительных глубоких научных исследований.

Список источников.

1. Digital-агентство WebCanape: Сайт. URL: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2024-v-mire-i-v-rossii/?utm_referrer=https%3a%2f%2fyandex.ru%2f

2. FOCA: программа. URL: https://foca.en.softonic.com/ Режим досупа: для зарегистрир.пользователей.

3. Shodan: поисковая система. URL: https://www.shodan.io Режим досупа: для зарегистрир.пользователей.

4. Securitylab.Ru: информационный портал по безопасности. URL: https://www.securitylab.ru/blog/personal/Neurosinaps/354501.php

5. EmailSherlock: программа. URL: https://www.emailsherlock.com

6. Search4faces: сервис поиска людей в интернете по фотографии. URL: https://search4faces.com

7. Карданов Р.Р., Никуличева И.В. Актуальные вопросы применения искусственного интеллекта для решения криминалистических задач // Вестник Сибирского юридического института МВД России. 2024. № 2 (55).

Информация об авторах:

А.А. Рясов,
профессор кафедры уголовного процесса и криминалистики
З.Р. Багиров,
старший преподаватель кафедры огневой подготовки

About the authors:

A.A. Ryasov, *Professor of the Department of Criminal Procedure and Forensic Science*

Z.R. Bagirov, *Senior Lecturer, Department of Fire Training*

Статья поступила в редакцию 14.01.2025