Грязнов Сергей Александрович
канд. пед. наук, доцент, декан
ФКОУ ВО «Самарский юридический институт ФСИН России»
г. Самара, Самарская область

ТЕНДЕНЦИИ И ВЫЗОВЫ ЦИФРОВОЙ КРИМИНАЛИСТИКИ

Аннотация: *статья представляет аналитический обзор современных тенденций и вызовов цифровой криминалистики, фокусируясь на изменении источников доказательств, эволюции методик сбора и анализа данных, а также правовых и организационных аспектах. Рассматриваются смещение акцента в сторону облачных и виртуализованных сред, внедрение методов машинного обучения и проблемы воспроизводимости выводов автоматизированных систем. Очерчены направления дальнейшего развития и практических мер, включающих эмпирическую валидацию методик, усиление правовой базы и подготовку междисциплинарных кадров.*

Ключевые слова: *цифровая криминалистика, облачные вычисления, стандартизация инструментов, защита персональных данных, блокчейн-криминалистика.*

В настоящее время цифровая криминалистика переживает этап ускоренной эволюции, вызванный многоплановой трансформацией информационных технологий и изменением поведенческих моделей пользователей. Ранее доминировавшее понятие «расследование цифровых преступлений, совершаемых с помощью отдельных устройств» постепенно уступает место более сложной картине, где источником доказательств становятся распределенные облачные сервисы, мобильные экосистемы, интернет вещей и многослойные сетевые инфраструктуры. Одновременно с этим увеличивается объем и разнообразие данных, растут требования к скорости реагирования и юридической устойчивости собранных материалов [1]. В этой связи видится актуальным аналитический обзор современных тенденций, инструментов и регуляторных практик, а также определение барьеров на пути становления цифровой криминалистики.

Первой и главной тенденцией является развитие облачной криминалистики. Здесь ключевые объекты исследований включают логи аутентификации и доступа, журналы событий сервисов (API-calls), снимки виртуальных дисков и памяти, метаданные объектов хранилищ, сетевую телеметрию. Перечень инструментов и практик сочетает международные коммерческие решения, отечественные продукты и свободно распространяемые утилиты, адаптированные под локальные реалии.

Так, для извлечения и анализа мультимедийных и пользовательских данных из мобильных устройств ранее широко применялся комплекс Belkasoft Evidence Center (российская компания BelkaSoft) [2], однако в 2022 году компания покинула российский рынок. Кроме того, из-за санкционного давления из России ушли многие зарубежные производители, например, израильская компания Cellebrite и швейцарская компания MSAB. Тем не менее в распоряжении силовых структур остались некоторые разработки, такие как «Мобильный криминалист» от компании «МКО-Системы», продукция компании Elcomsoft, а также китайское решение Forensic MagiCube. Подобные технологии позволяют установить, где находился человек в конкретный момент времени, а также выявить связи между подозреваемыми, если они оказывались в одном месте. Однако временная синхронизация является острой проблемой облачной криминалистики. В распределенных системах источники логов могут иметь различную точность временных меток, что требует четкой нормализации времени при корреляции событий. Также вызовом является необходимость верификации происхождения данных – документирование цепочки получения через API, запросы к поддержке провайдера и сохранение подписанных экспортов для судебной пригодности.

Вторая тенденция – машинное обучение и искусственный интеллект (ИИ). В прикладных процессах ИИ применяется для автоматизации триажа и приоритизации материалов, распознавания биометрии, обнаружения аномалий в логах и сетевой телеметрии, а также для обработки документов и трассировки транзакций в блокчейне – это повышает оперативность, но требует тщательной ве-

рификации результатов. В российской практике основу технической экосистемы составляют инструменты компьютерного зрения и аудиоанализа, ELK-стек и коммерческие SIEM-решения, а также отечественные продукты биометрии и кибераналитики. Ограничивающими факторами здесь являются правовые требования к персональным и биометрическим данным, дефицит репрезентативных и юридически пригодных обучающих наборов, уязвимость моделей к adversarial-приемам (преднамеренные манипуляции с входными данными) и возможные смещения, приводящие к систематическим ошибкам. Следовательно, судебная пригодность выводов на базе ИИ требует протоколов валидации, воспроизводимости и прозрачной документации, включая логирование данных, версионирование моделей и обязательное участие эксперта на финальном этапе.

Третья тенденция – развитие блокчейн-технологий, которые изменили природу финансовых и информационных следов – сделали их публичными в новом формате и одновременно породили уникальные вызовы по установлению субъектности и контекста транзакций. В криминалистике появился новый тип первичных артефактов – цепочки транзакций и графы взаимодействий, которые можно анализировать для восстановления последовательности, например, денежных переводов, и выявления закономерностей поведения адресов, обнаруживая паттерны, типичные для отмывания средств или финансирования преступной деятельности. Внутри профессиональных криминалистических команд появились новые специализации: on-chain аналитики, эксперты по смарт-контрактам, специалисты по взаимодействию с площадками обмена и юридические консультанты по вопросам криптовалютного права. В 2021 г. Федеральная служба по финансовому мониторингу Российской Федерации представила программное обеспечение под названием «Прозрачный блокчейн», созданное на базе ИИ. Данное программное обеспечение призвано решить следующие задачи: отслеживать цепочки перемещений цифровых финансовых активов; осуществлять мониторинг поведения участников криптовалютного рынка с целью их идентификации; вести базу данных криптовалютных кошельков, связанных с осуществлением противоправной деятельности и фи-

нансированием терроризма; составлять профили участников крипторынка и оценивать их роль в экономической деятельности; выявлять вероятность их участия в противоправной деятельности [3]. Таким образом, блокчейн-криминалистика вступила в динамичную фазу развития вследствие постоянного появления новых технологий и моделей злоупотреблений. Перспективы дальнейшего развития включают усиление междисциплинарного подхода, развитие стандартов верификации on-chain доказательств и усиление сотрудничества между государственными органами, биржами и аналитическими провайдерами.

Наконец, проблемы и перспективы развития научной и педагогической составляющих отрасли. современный преподаватель криминалистики должен обладать глубокими теоретическими знаниями в области криминалистики, а также иметь личный практический опыт в сфере противодействия преступности. Такая двухуровневая формула преподавателя обеспечит как предоставление аудитории необходимого качественного набора криминалистических знаний, так и обезопасит авторитет преподавателя. Такой уровень профессиональной криминалистической подготовки достигается в процессе обучения в аспирантуре (адъюнктуре), а также при прохождении преподавателем обязательного курса повышения квалификации (на системной и плановой основе) в правоохранительных органах, суде или экспертно-криминалистических лабораториях (в том числе цифровых). Нехватка квалифицированных кадров, необходимость междисциплинарного набора знаний и постоянное обновление компетенций стимулируют появление специализированных курсов, моделей сертификации и коллаборативных платформ для обмена опытом. При этом образовательные программы должны фокусироваться не только на инструментах, но и на методологии, правовой грамотности и вопросах этики, что повысит качество работы и юридическую устойчивость выводов.

Обобщая вышеизложенное, можно констатировать что технические инновации открывают новые возможности для выявления и анализа цифровых преступлений, но одновременно порождают сложные вызовы, связанные с масшта-

бом данных, распространением шифрования и применением антикриминалистических приемов. Адекватный ответ на эти вызовы требует комплексного подхода, объединяющего развитие методов сбора и анализа, стандартизации инструментов, усиления юридической и этической базы, а также инвестиций в человеческий капитал. Таким образом, стратегическая задача отрасли видится в обеспечении воспроизводимости и объяснимости выводов при одновременном уважении прав на приватность.

Список литературы

1. Григорьев А.Н. Развитие «цифровой криминалистики» как необходимое условие обеспечения цифрового суверенитета Российской Федерации / А.Н. Григорьев // Современные технологии и подходы в юридической науке и образовании: сборник материалов Междунар. науч.-практ. форума (Калининград, 27–31 августа 2020 г.). – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. – С. 254–261.

2. Соколова А.В. Цифровая обработка криминалистически значимой информации на примере судебно-баллистической экспертизы / А.В. Соколова // Вестник Уфимского юридического института МВД России. – 2025. – №3 (109). – С. 91–101. EDN PKOOLT

3. Чихрядзе А.М. Система блокчейн: криминалистический аспект / А.М. Чихрядзе // Философия права. – 2024. – №3 (110). – С. 187–192. EDN XZUBFL