В области высшего образования статистика также впечатляет. Исследование, проведенное в одном из американских университетов, показало, что процент студентов, успешно сдавших экзамен и использующих систему обучения на базе ИИ, увеличился на 12% по сравнению с контрольной группой. Эти данные легко найти в открытом доступе по запросам. «Статистика эффективного обучения, используя ИИ» или «Адаптивное обучение студентов через ИИ» в базах данных научных публикаций.

Таким образом, искусственный интеллект трансформирует подход к решению проблемы академической неуспеваемости, предоставляя двоечнику не просто доступ к информации, а комплексную систему для персонализированной работы над ошибками. От адаптивных платформ, выстраивающих индивидуальную образовательную траекторию, до интеллектуальных репетиторов, объясняющих конкретные недочеты, и систем интервального повторения для эффективного запоминания – арсенал инструментов ИИ позволяет системно и точечно ликвидировать пробелы в знаниях. Статистические данные и конкретные примеры внедрения подтверждают, что использование данных технологий ведет к значительному повышению успеваемости, сокращению времени на освоение материала и, что самое важное, формированию устойчивой мотивации к обучению у ранее отстававших учащихся.

Бригадирова К.В.

Волгоградская академия МВД России

Информационно-коммуникационные технологии как новая реальность расследований: стратегии трансформации криминалистической подготовки

Современная преступность все глубже уходит в цифровое пространство. Смартфоны, мессенджеры, социальные сети, облачные сервисы и другие информационно-телекоммуникационные технологии (далее – ИКТ), ставшие неотъемлемой частью повседневной жизни законопослушного гражданина, активно используются и в преступных целях от организации наркооборота и вербовки в экстремистские группы до совершения кибермошенничества. Эта трансформация привела к радикальному изменению следообразующей среды: вместо материальных улик все чаще остаются цифровые артефакты: метаданные, цифровые журналы, геолокационные отметки. В этих условиях эффективность правоохранительной деятельности напрямую зависит от способности сотрудников органов внутренних дел адекватно воспринимать, извлекать, анализировать и использовать информацию, порождаемую ИКТ.

Целью нашего обсуждения стоит обоснование необходимости системной трансформации криминалистических знаний и методик как ключевого условия успешного расследования в эпоху цифровой преступности, а следовательно, и подходов при подготовке будущих специалистов для органов внутренних дел. Необходимо понимать, что без обновления образовательных программ, методологических основ и практических навыков правоохранительные органы рискуют оказаться в состоянии «цифрового отставания», что напрямую скажется на раскрываемости преступлений и защите общественной безопасности.

Современные информационно-телекоммуникационные технологии в контексте правоохранительной деятельности выполняют двойственную функцию: они одновременно выступают объектом расследования, когда используются для совершения преступлений, и средством расследования, когда задействуются оперативными и следственными органами для сбора доказательств, установления личности и восстановления картины происшествия. Эта двойственность требует от сотрудников ОВД не только технической грамотности, но и четкого понимания правовых и методологических границ применения цифровых инструментов.

В случаях, когда преступления совершаются с использованием смартфонов, мессенджеров, социальных сетей или иных цифровых платформ, сами устройства и сервисы становятся источниками криминалистически значимой информации. Цифровые следы, такие как метаданные сообщений, журналы вызовов, геолокационные данные, история посещений сайтов, временные метки файлов, позволяют реконструировать хронологию событий, установить связи между участниками преступной группы и выявить мотивы деяний. Однако работа с такими следами сопряжена с рядом сложностей. Во-первых, данные часто фрагментированы: часть информации хранится на устройстве подозреваемого, часть на серверах провайдеров или в облачных хранилищах, доступ к которым ограничен юрисдикционными и техническими барьерами. Во-вторых, все чаще используются сквозное шифрование, самоуничтожающиеся сообщения и анонимайзеры, что затрудняет или делает невозможным получение содержательной информации даже при наличии законных оснований. В-третьих, изъятие и фиксация цифровых доказательств требуют соблюдения строгих процедур, иначе доказательства могут быть признаны недопустимыми в суде.

С другой стороны, ИКТ становятся мощным инструментом в руках следователей и оперативных работников. Современные расследования все чаще опираются на открытые источники (OSINT), анализ сетевой активности, мониторинг публичных аккаунтов в соцсетях, использование геоаналитики и даже искусственного интеллекта для выявления паттернов поведения отдельных граждан.

Традиционные криминалистические методики, разработанные в эпоху преимущественно «офлайн»-преступности, все чаще оказываются недостаточными для эффективного расследования деяний, совершенных в цифровой среде. Это обусловлено не только изменением форм преступного поведения, но и фундаментальным сдвигом в природе следов: от материальных (следы пальцев рук, подошв обуви, ДНК) к виртуальным (IP-адреса, цифровые подписи, журнальные лог-файлы). В ответ на эти вызовы криминалистика, как наука и практика, проходит этап глубокой трансформации, направленной на интеграцию цифровых подходов в существующие методологические рамки. Согласимся со мнением В.А. Попова: «…отметим необходимость совершенствования тактики следственных действий, позволяющих в кратчайшие сроки получить доступ к цифровым следам преступлений на машинных носителям информации, грамотно работать с ними, наконец, использовать в качестве вещественных доказательств, изобличающих виновных»[1].

Современные расследования все чаще требуют применения специализированных видов экспертиз, выходящих за пределы классической криминалистики. Наиболее востребованными становятся компьютерно-техническая экспертиза, позволяющая извлекать и анализировать данные с электронных устройств; лингвистическая экспертиза, направленная на установление авторства текстов в мессенджерах или соцсетях; а также реконструкция в ходе исследований маршрутов передачи данных и выявление анонимных аккаунтов. Особое значение приобретают методы, основанные на анализе больших данных при помощи искусственного интеллекта: алгоритмы машинного обучения позволяют автоматически классифицировать изображения, выявлять связи между участниками преступных сообществ по особенностям их коммуникации или предсказывать вероятные места совершения преступлений на основе зафиксированных ранее данных.

Несмотря на технологический прогресс, внедрение новых методик сталкивается с рядом системных барьеров. Во-первых, методологическая база криминалистики развивается медленнее, чем меняется технологическая реальность. Многие цифровые следы до сих пор не имеют четко регламентированных процедур фиксации, изъятия и оценки, что создает риски признания доказательств недопустимыми. Во-вторых, нормативно-правовая база часто отстает от практики: например, законодательство не всегда учитывает особенности облачных сервисов, мессенджеров, содержащих шифрование или децентрализованных платформ (например, блокчейн-сетей). В-третьих, существует разрыв между теорией и практикой: даже при наличии совре-

[1] Попов В.А., Рудавин А.А. Тактика следственного осмотра по делам о преступлениях в сфере компьютерной информации // Сборник научных статей по итогам Недели российской науки в Рязанском филиале Московского университета МВД России имени В.Я. Кикотя, Рязань, 1-8 февраля 2023 года. Рязань: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2023.

менных инструментов участники предварительного следствия нередко не обладают достаточной квалификацией для их эффективного применения, а экспертные учреждения испытывают дефицит кадров с междисциплинарной подготовкой.

Эффективное противодействие цифровой преступности невозможно без соответствующей подготовки личного состава. Если еще десятилетие назад знание основ криминалистики и уголовного процесса считалось достаточным для большинства сотрудников ОВД, занимающихся выявлением и расследованием преступлений, то сегодня от них требуется гибридная компетентность, сочетающая юридическую, криминалистическую и цифровую грамотность. Эта трансформация требует как обновления системы начального профессионального образования, так и создания устойчивой системы непрерывного обучения.

Современный сотрудник ОВД должен уметь не только правильно оформить процессуальный документ, но и понимать, как извлекаются метаданные из изображения, что такое цепочка хранения цифровых доказательств, как работает геолокация через сотовые вышки или почему мессенджер с оконечным шифрованием ограничивает доступ к содержанию переписки. Это не означает, что каждый следователь или эксперт должен становиться программистом, но базовое понимание архитектуры цифровых систем, принципов работы сетей и особенностей хранения данных становится обязательным. Кроме того, возрастает роль навыков взаимодействия со специалистами: сотрудник должен уметь грамотно сформулировать вопросы для цифровой экспертизы, интерпретировать ее выводы и интегрировать их в общую доказательственную стратегию.

Формирование таких компетенций невозможно в рамках узкоспециализированной подготовки. Требуется междисциплинарная интеграция: курсы по основам информационной безопасности, цифровой криминалистики, анализа данных и даже основ искусственного интеллекта должны органично вписываться в учебные планы при подготовке будущих сотрудников ОВД. Особенно перспективным является сочетание криминалистики с элементами, содержащими анализ цифровых следов. Такой подход позволяет не просто «реагировать» на новые технологии, а прогнозировать их криминальное использование и разрабатывать активные методы противодействия и профилактики[1].

Образовательные учреждения системы МВД должны стать локомотивами этой трансформации. Без системной работы в этом направлении даже самые передовые технологии окажутся бесполезными – из-за отсутствия

[1] Коробкова Е.А. Использование специальных знаний при расследовании преступлений в сфере информационных технологий // Молодежная инициатива : сборник статей IX международной научно-практической конференции, Пенза, 15 мая 2025 года. Пенза: Пензенский государственный аграрный университет, 2025. С. 52-59.

кадров, способных их грамотно применять в рамках закона и методологии, а следовательно, накапливать опыт и проверять имеющиеся научно-методические наработки.

Цифровая трансформация общества неизбежно влечет за собой трансформацию преступности и, как следствие, трансформацию криминалистики. Информационно-телекоммуникационные технологии уже не просто «инструмент» преступников, а среда, в которой формируются новые преступные деяния, стираются традиционные границы между преступлением и его последствиями, а также возникают принципиально иные типы доказательств. В этих условиях криминалистика перестает быть исключительно прикладной юридической дисциплиной и превращается в междисциплинарную область, требующую синтеза знаний из права, информатики, технологий и анализа данных.

Ключевым фактором адаптации правоохранительной системы к этим вызовам становится человеческий потенциал: сотрудники ОВД должны обладать не только правовой и следственной культурой, но и цифровой грамотностью, позволяющей уверенно ориентироваться в сложной ИКТ-среде. Без системной, научно обоснованной и опережающей модернизации криминалистических знаний и компетенций сотрудников эффективность борьбы с преступностью в цифровую эпоху будет неизбежно снижаться. Поэтому трансформация криминалистики – это не опциональный тренд, а насущная необходимость, определяющая будущее правоохранительной деятельности.

Сигерич М.Я.

Волгоградская академия МВД России

Возможности назначения криминалистических экспертиз по записям и подписям, выполненным на электронных устройствах с сенсорным экраном

Современные сенсорные устройства, от смартфонов до специализированных графических планшетов, все чаще используются для создания рукописных записей и подписей в гражданском, административном и уголовном обороте. Переход от традиционного бумажного носителя к цифровой среде трансформирует саму природу объекта исследования, подходы к его оценке. В этих условиях возникает необходимость разграничения видов криминалистических экспертиз, применимых к таким объектам, выработки требований к их назначению. Понимание того, какие экспертизы возможны, какие вопросы они способны решить и какие условия необходимы для получения выводов, становится ключевым фактором эффективного правоприменения. В этой связи особую актуальность приобретают вопросы корректного опреде-