Хачатрян Артем Еремович
бакалавр, студент
Кочнев Артем Алексеевич
студент
Миллер Арина Владиславовна
преподаватель
ФГБОУ ВО «Кубанский государственный аграрный
университет им. И.Т. Трубилина»
г. Краснодар, Краснодарский край

ВЛИЯНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ НА ПРОЦЕСС РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ: ПРАВОВЫЕ НОРМЫ, ТАКТИЧЕСКИЕ ПРИЁМЫ И ЭТИЧЕСКИЕ ДИЛЕММЫ

Аннотация: *в статье рассматривается комплексное влияние научно-технического прогресса на судебно-экспертную деятельность. Основное внимание уделяется легитимизации электронных доказательств, трансформации тактики расследования и разрешению этических конфликтов, возникающих при внедрении высоких технологий в уголовный процесс.*

Ключевые слова: *цифровая трансформация, Уголовно-процессуальный кодекс Российской Федерации, электронные следы, киберпреступность, тактика ведения допроса, искусственный интеллект, права человека.*

Глобальная цифровизация общественных коммуникаций привела к виртуализации преступной деятельности, что обусловило необходимость анализа правовых норм, тактики и этических дилемм, возникающих в ходе расследований. Согласно статистике МВД России, за 2024 год было зарегистрировано 765,4 тыс. киберпреступлений за 11 месяцев, каждое четвертое преступление в стране совершалось с использованием информационно-коммуникационных технологий с 2020 года это максимальный показатель. В 2025 году число IT-преступлений сократилось почти на 12%, на 4,6% сократилось количество тяжких и особо тяжких преступлений в сфере информационно-коммуникационных технологий.

Количество дистанционных краж снизилось на 23,6%, дистанционных мошенничеств – на 9%, а преступлений в сфере компьютерной информации – на 42,2%. В этих условиях традиционная криминалистическая парадигма, ориентированная в первую очередь на материально зафиксированные следы, претерпевает радикальную трансформацию. Появление термина «цифровая криминалистика» свидетельствует о формировании новой отрасли науки, изучающей закономерности появления, поиска, фиксации и исследования информации в цифровой среде. Однако внедрение технологий в следственную практику опережает темпы законодательного регулирования, создавая правовые пробелы и этические конфликты.

Уголовно-процессуальное законодательство РФ регулирует использование информационных технологий, но имеет ряд пробелов. Ключевое нововведение – ст. 164.1 УПК РФ, которая устанавливает особый порядок изъятия электронных носителей информации [1] Закон требует обязательного участия специалиста, что обусловлено уязвимостью цифровой информации: её легко удалить или изменить.

Однако процессуальный статус самой цифровой информации остается неопределенным. Возникает вопрос, является ли она «вещественным доказательством» (статья 81 УПК РФ) или «иным документом» (статья 84 УПК РФ)? Проблема в том, что вещественные доказательства по своей сути неизменяемы и привязаны к физической подложке, в то время как цифровая информация может быть скопирована без потери своих свойств, что противоречит классической концепции уникальности вещественного доказательства [5]

Трансграничный характер данных создает дополнительные сложности. Улики часто хранятся не на физическом диске компьютера подозреваемого, а в «облачных» системах хранения, серверы которых расположены в иностранных юрисдикциях. Действующие положения УПК РФ о международном сотрудничестве (глава 53) предполагают длительный процесс запроса, который несовместим со скоростью уничтожения данных в интернете. Требуется разработка правовых механизмов для немедленного трансграничного доступа к данным в экстренных случаях [4].

Раньше стандартным методом выключения компьютера было экстренно отключить сетевой кабель («выдернуть вилку из розетки»), но эта практика утратила свою эффективность. Завершение работы системы таким образом приводит к потере содержимого оперативной памяти, которая является важной областью для хранения временных данных. Потеря этих данных означает потерю ключей шифрования, активных сообщений, следов вредоносных процессов и записей об удаленных подключениях [6].

Современный метод предполагает поддержание устройства в рабочем состоянии и использование специализированного программного обеспечения для безопасного извлечения данных из оперативной памяти. Этот процесс должен выполняться экспертами в присутствии независимых наблюдателей и специалиста для обеспечения точности и целостности процесса извлечения данных.

Современное место происшествия заполнено техническими устройствами: умными часами, фитнес-браслетами, IP-камерами и даже бытовой техникой. Тактика осмотра места происшествия теперь включает обязательную проверку сетевых подключений. Данные о частоте сердечных сокращений жертвы, полученные с помощью фитнес-браслета, позволяют определить точное время смерти с точностью до минут, а логи «умного дома» могут предоставить информацию о передвижениях преступника по помещению.

3D-сканирование все чаще используется в тактике следственных экспериментов и осмотров мест преступлений. Это позволяет создать цифровую копию места преступления, по которому участники судебного процесса могут виртуально попасть на место преступления спустя время после происшествия. Это значительно уменьшает риск потери информации о месте происшествия из-за погодных условий или деятельности человека.

Допросу подозреваемого теперь предшествует глубокий анализ его цифрового следа (следы, которые человек оставляет в процессе пользования интернетом или цифровыми технологиями). Изучение активности в социальных сетях, истории поисковых запросов и геолокации позволяет следователю применять тактику, основанную на знании скрытых сторон жизни допрашиваемого, что

способствует более быстрому установлению психологического контакта или разоблачению лжи.

Использование высоких технологий в уголовном процессе неизбежно затрагивает сферу фундаментальных прав человека, порождая острые этические споры. Например, согласно статье 51 Конституции России, никто не обязан свидетельствовать против самого себя, ст. 23 Конституции РФ (право на тайну переписки и телефонных переговоров) [1] Возникает вопрос, является ли принудительное прикладывание пальца подозреваемого к сканеру смартфона или сканирование его лица (FaceID) нарушением этих норм? С одной стороны, это является приемлемым способом получения «образцов для сравнительного исследования» (по аналогии с отпечатками пальцев). С другой стороны, смартфон является это цифровое продолжение личности, хранящее сокровенные мысли и переписку, и доступ к нему без согласия владельца равносилен принудительному допросу. Четкие рамки принудительной и добровольной биометрии оформились относительно недавно, в связи с принятием Закона №572-ФЗ и дополнением ст. 11 Закона №152-ФЗ и ч. 3 Закона №572-ФЗ [7].

Внедрение систем искусственного интеллекта для анализа больших данных позволяет прогнозировать вероятность совершения преступлений определенными лицами. Этический риск заключается в подмене принципа презумпции невиновности теоретической и статистической вероятностью виновности. Существует опасность того, что следствие будет предвзято относиться к конкретному лицу только потому, что алгоритм отметил его как склонного к рецидивам. Право на гуманное судебное решение является фундаментальным этическим требованием современного законодательства.

Системы распознавания лиц и повсеместное видеонаблюдение значительно облегчают поиск преступников на месте. Однако это снижает право граждан на неприкосновенность частной жизни. Этический баланс между общественной безопасностью и правом на неприкосновенность частной жизни остается широко обсуждаемой темой в области права.

Основываясь на анализе влияния технологий на процесс расследования, необходимо внести ряд изменений в правовую базу.

1. Законодательно закрепить понятие «цифровая информация» как самостоятельный объект, отличный от вещественных доказательств и документов [3].

2. Разработать регламент удаленной проверки данных в облачных хранилищах, с установлением четких границ для вмешательства в частную жизнь и процедуры получения судебного разрешения.

3. Легализовать использование нейронных сетей в криминалистических целях (например, для восстановления изображений с камер видеонаблюдения) при условии создания прозрачной методологии проверки точности работы алгоритмов и верификации результатов независимыми экспертами.

4. Создание стандартов «цифровой этики» для сотрудников правоохранительных органов, которые исключают использование полученных данных в целях, не связанных с интересами правосудия.

Влияние современных технологий на расследование преступлений имеет как положительные, так и отрицательные стороны. С одной стороны, правоохранительные органы получили беспрецедентные инструменты для раскрытия самых сложных и малоизвестных преступлений. С другой стороны, существует риск подрыва установленных процессуальных гарантий прав личности. Вместо того чтобы превращаться в цифровую инквизицию, технологии должны расширять интеллектуальные и технические возможности правосудия, не подрывая его фундаментальных принципов.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 №174-ФЗ.

3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ.

4. Криминалистика: учебник для вузов / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская. – М.: Норма, 2026.

5. Мамонтов А.Г. Цифровая криминалистика: от истоков к современному состоянию / А.Г. Мамонтов // Право и государство: теория и практика. – 2020. – №12 (192).

6. Пастухов П.С. Цифровые платформы как основа электронного документооборота в уголовном судопроизводстве / П.С. Пастухов // Пермский юридический альманах. – 2023. – №6. EDN LNGSYX

7. Митянов З.О. Принудительная и добровольная биометрия: содержание и разграничение в российском праве / З.О. Митянов // Теоретическая и прикладная юриспруденция. – 2024. – №3 (21).