УДК 343

ПРОБЛЕМА ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ВЫЯВЛЕНИЯ И РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ

Кириченко О.А.

студент,

Белгородский государственный национальный исследовательский университет,

Белгород, Россия

Романенко В.Н.

студент,

Белгородский государственный национальный исследовательский университет,

Белгород, Россия[1]

Аннотация: В статье рассматриваются проблемы использования информационных технологий при выявлении и раскрытии преступлений. Систематизируются основные направления их применения: базы данных и СПИС, анализ социальных сетей и соединений абонентов, биометрическая идентификация, технологии искусственного интеллекта. Анализируется нормативная база применения ИИ. Выделены ключевые проблемы: отсутствие легального определения электронного доказательства, обеспечение подлинности цифровых доказательств, риски нарушения прав граждан, ошибки алгоритмов и дефицит компетенций сотрудников. Автор приходит к выводу, что проблема заключена не в самих технологиях, а в их несистемном и фрагментарном применении.

Ключевые слова: информационные технологии, выявление и раскрытие преступлений, электронные доказательства, цифровые следы, искусственный интеллект, правовое регулирование, информационная безопасность.

[1]Научный руководитель: Ярощук И.А., к.филол.н., доцент, и.о. заведующего кафедрой судебной экспертизы и криминалистики, Белгородский государственный национальный исследовательский университет, Белгород, Россия

THE PROBLEM OF USING INFORMATION TECHNOLOGIES TO IDENTIFY AND SOLVE CRIMES

Kirichenko O.A.

student,

Belgorod State National Research University,

Belgorod, Russia

Romanenko V.N.

student,

Belgorod State National Research University,

Belgorod, Russia[2]

Abstract: The article examines the problems associated with using information technologies in detecting and solving crimes. The main areas of their application are systematized: databases and SPIS, analysis of social networks and subscriber connections, biometric identification, and artificial intelligence technologies. The regulatory framework for the use of AI is analyzed. Key problems are identified: the lack of a legal definition of electronic evidence, ensuring the authenticity of digital evidence, risks of violating citizens' rights, algorithmic errors, and a lack of staff competencies. The author concludes that the problem lies not in the technologies themselves, but in their unsystematic and fragmented application.

Keywords: information technology, crime detection and investigation, electronic evidence, digital traces, artificial intelligence, legal regulation, information security.

Развитие цифровых форм преступной деятельности определяет использование информационных технологий неизбежным требованием. Цифровые следы сегодня сопровождают практически любое преступление,

[2]Scientific supervisor: Yaroshchuk I.A., Candidate of Philological Sciences, Associate Professor, Acting Head of the Department of Forensic Science and Criminalistics, Belgorod State National Research University, Belgorod, Russia.

поэтому отказ от IT-инструментов в этих условиях означал бы добровольный отказ от значительной части доказательственной базы. Сейчас информационные технологии превратились в условие результативности деятельности по выявлению и раскрытию преступлений.

Легальное содержание понятия «информационные технологии» раскрывается в ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», где под ними понимаются «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов» [1]. В доктрине предлагаются и более развёрнутые дефиниции. Так, например, В.В. Фролов определяет информационные технологии в расследовании как «совокупность приемов и методов сбора, обработки, хранения, представления и использования криминалистически значимой информации, с применением специальных средств (компьютеры, ноутбуки, смартфоны, программное обеспечение, компьютерные сети и др.), направленных на принятие следователем организационных, тактических и методических решений с их последующей реализацией, обеспечивающей достижение целей расследования» [2].

Применение информационных технологий в деятельности по выявлению и раскрытию преступлений развивается по нескольким взаимосвязанным направлениям, каждое из которых обладает собственной спецификой.

Наиболее традиционным и вместе с тем постоянно совершенствующимся направлением остаётся использование специализированных баз данных и справочно-информационных систем (СПИС).Оно реализуется через автоматизированные информационные системы унифицированного характера, предполагающие хранение дактилоскопической, геномной и иной информации, в том числе следов биологического происхождения, в форме баз данных. Такие системы позволяют установить личность предполагаемого преступника в течение минимально короткого

промежутка времени либо сопоставить различные эпизоды противоправной деятельности в целях выявления их схожести. В качестве иллюстрации можно привести информационную систему «СПРУТ», посредством которой формируются учёты и обеспечивается контроль за раскрытием преступлений [3].

Логическим продолжением работы с информационными массивами становится анализ социальных сетей и интернет-ресурсов как источника ориентирующей информации. Исследования показывают, что социальные сети всё чаще используются для поиска криминалистически значимой информации.

Отдельного внимания заслуживает метод анализа данных об интернет-соединениях между абонентами. Анализ сведений о соединениях абонентов между собой и с базовой станцией сегодня рассматривается как один из наиболее перспективных способов получения ориентирующей информации. Он позволяет установить траекторию перемещения лица, его местонахождение в конкретный момент времени, а также круг лиц, с которыми оно вступало в контакт накануне совершения преступления [4]. Цифровые следы, оставляемые пользователями в сети, становятся самостоятельным объектом криминалистического исследования, требующим специальных познаний и методик. Вместе с тем именно это направление наиболее тесно соприкасается с конституционным правом на неприкосновенность частной жизни и тайну переписки, что требует особой тщательности в вопросах процессуального оформления.

Стоит отметить, что возможности информационных технологий не ограничиваются поиском и анализом данных, они всё чаще позволяют идентифицировать человека по его уникальным физическим параметрам. Показателен пример системы распознавания лиц FindFace (NtechLab), которая с точностью более 99,9% позволила в Архангельской области найти 45 без вести пропавших и поспособствовала раскрытию свыше 300 преступлений [5].

Следственный комитет РФ применяет самостоятельно разработанные системы распознавания лиц и анализа цифровых следов для эффективного расследования киберпреступлений, технологии внедрены в специализированном подразделении Главного следственного управления по расследованию киберпреступлений. Кроме того, в системе Следственного комитета проходит апробацию комплекс «Детектив», позволяющий осуществлять двухканальную запись и транскрибацию диалога [6].

Наиболее динамично развивающимся направлением выступают технологии искусственного интеллекта (ИИ) в следственной деятельности. Под ИИ в доктрине понимается «создаваемое с помощью группы смежных технологий программное обеспечение, функционирующее нелинейно, способное к обучению, ограниченному пониманию причинности и выполнению задач интеллектуального, эвристического характера с возможностью обучения, корректировки и уточнения за счет опыта принимаемых решений» [7].Возможности ИИ существенно расширяют потенциал следственных действий, так как системы машинного обучения позволяют анализировать большие объёмы данных для выявления паттернов преступной деятельности и идентификации правонарушителей. Стоит отметить, что внедрение ИИ в правоохранительную деятельность требует обзора нормативно-правовой основы, поскольку возможности ИИ существенно расширяют возможности следственных действий, но одновременно порождают вопросы, связанные с допустимостью получаемых результатов.

Нормативная база применения ИИ в правоохранительной деятельности формируется комплексно. Ключевым актом здесь выступает Федеральный законот 28.06.2014 N 172-ФЗ«О стратегическом планировании в РФ» [8]; важную роль играют указы Президента о национальных целях развития, стратегии развития информационного общества на период до 2030 года и научно-технологического развития страны. Особое значение имеет Национальная стратегия развития искусственного интеллекта до 2030 года (с

изменениями 2024 года) [9], в которой закреплены фундаментальные принципы, приоритетные направления, целевые показатели и механизмы поддержки развития ИИ, а обеспечение правопорядка прямо названо одним из приоритетных направлений внедрения соответствующих технологий.

Таким образом, рассмотренные направления демонстрируют значительный потенциал информационных технологий. Однако их практическая реализация сталкивается с комплексом взаимосвязанных проблем.

Наиболее фундаментальной остаётся проблема правовой регламентации электронных доказательств. В Уголовно-процессуальном кодексе РФ отсутствует легальное определение «электронного доказательства», что порождает оживлённую дискуссию о его месте в системе доказательств. Перечень видов доказательств, закреплённый в ч. 2 ст. 74 УПК РФ, является закрытым и не включает электронные доказательства в качестве самостоятельного вида, за последние десятилетия этот перечень не претерпевал изменений, несмотря на появление и активное развитие новых объектов, способных выступать доказательствами по уголовному делу [10].

При этом важно подчеркнуть, что правовая основа для применения информационных технологий в целом создана. Нормативными правовыми актами, регулирующими деятельность по выявлению и раскрытию преступлений, возможность использования информационных технологий закреплена прямо. Так, статья 6 Федерального законаот 12.08.1995 N 144-ФЗ«Об оперативно-розыскной деятельности» допускает применение информационных систем при производстве оперативно-розыскных мероприятий [11]. Более того, отдельные оперативно-розыскные мероприятия, прежде всего получение компьютерной информации, в принципе не могут быть осуществлены без использования информационных технологий. Таким образом, практическая деятельность обеспечена нормативной основой, тогда как процессуальный статус её результатов остаётся неопределённым.

Кроме того, особую остроту приобретает проблема сохранения подлинности доказательств, полученных цифровым способом. В электронный файл, в отличие от физического объекта, достаточно несложно внести изменения, а потому возникает потребность в технологиях, гарантирующих неизменность данных с момента их изъятия.

Не менее серьёзен вопрос обеспечения информационной безопасности и соблюдения прав граждан. В целях раскрытия и расследования преступлений в распоряжении правоохранительных органов накапливается значительный массив персональной информации, при этом естественным образом возникают риски её неправомерного использования или утраты.Конституционная значимость этой проблемы подчёркивается в п. «м» ст. 71 Конституции РФ, относящем к ведению Российской Федерации «обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных» [12]. Проблема, таким образом, заключена не в самих технологиях, а в их несистемном и фрагментарном применении. Возникает необходимость обеспечения баланса между эффективностью раскрытия преступлений и правом на неприкосновенность частной жизни.

Кроме того, внедрение автоматизированных систем создаёт риски ошибок алгоритмов и зависимости следствия от технических сбоев. Проблема верифицируемости результатов, получаемых с помощью ИИ, напрямую связана с вопросом о допустимости таких результатов в качестве доказательств. Ошибка алгоритма, не выявленная своевременно, способна привести к получению недопустимых доказательств и, как следствие, к нарушению прав участников уголовного процесса.

Отдельного внимания заслуживает проблема, которую можно обозначить как кадровую. Ряд сотрудников правоохранительных органов не обладает достаточными компетенциями в вопросах использования информационных технологий. Незнание потенциала современных

информационных инструментов существенно тормозит процесс расследования отдельных категорий преступлений, особенно совершённых в сфере компьютерной информации [4].

Таким образом, применение информационных технологий в деятельности по выявлению и раскрытию преступлений является объективной необходимостью, обусловленной цифровизацией самой преступности. Вместе с тем их практическая реализация сталкивается с комплексом взаимосвязанных правовых, организационных и кадровых проблем, которые не позволяют в полной мере использовать имеющийся потенциал.Правоохранительные органы сегодня должны не просто успевать за техническим прогрессом, а опережать преступный мир в освоении современных технологий.

Библиографический список:

1. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ. — 2006. — № 31 (ч. I). — Ст. 3448.

2. Фролов В. В. Использование информационных технологий в расследовании: направления, проблемы и перспективы //Полицейская и следственная деятельность. – 2023. – №. 2. – С. 1-13.

3. Иконников Д. С., Ковалев О. Г. Правовые и организационные особенности применения современных информационных технологий и поисковых систем розыска осужденных, уклоняющихся от отбывания наказания без изоляции от общества //Право и управление. – 2024. – №. 7. – С. 335-339.

4. Грицаев С. И., Дулепина О. В. Проблемы использования информационных технологий для выявления и раскрытия преступлений //Полицейская деятельность. – 2025. – №. 5. – С. 131-144.

5. В РФ предотвратили сотни преступлений и нашли пропавших без вести с помощью ИИ // Газета.Ru. — 2025. — 30 октября. —

URL: https://www.gazeta.ru/tech/news/2025/10/30/27067412.shtml (дата обращения: 06.11.2026).

6. Официальный сайт Следственного комитета Российской Федерации : новости. — URL: https://sledcom.ru/news/item/1984087/ (дата обращения: 07.11.2026).

7. Степаненко Д. А., Бахтеев Д. В., Евстратова Ю. А. Использование систем искусственного интеллекта в правоохранительной деятельности //Всероссийский криминологический журнал. – 2020. – Т. 14. – №. 2. – С. 206-214.

8. О стратегическом планировании в Российской Федерации : Федеральный закон от 28.06.2014 № 172-ФЗ // Собрание законодательства РФ. — 2014. — № 26 (ч. I). — Ст. 3378.

9. О развитии искусственного интеллекта в Российской Федерации : Указ Президента РФ от 10.10.2019 № 490 (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства РФ. — 2019. — № 41. — Ст. 5700.

10. Никурадзе Н. О., Мищенко Е. В., Марина Е. А. «Электронные доказательства»: о понятии и правовом регулировании в свете потребностей практики раскрытия и расследования преступлений (российский и зарубежный опыт) // Всероссийский криминологический журнал. 2025. №6.

11. Об оперативно-розыскной деятельности : Федеральный закон от 12.08.1995 № 144-ФЗ // Собрание законодательства РФ. — 1995. — № 33. — Ст. 3349.

12. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6–ФКЗ, от 30.12.2008 № 7–ФКЗ, от 05.02.2014 № 2–ФКЗ, от 01.07.2020 № 11–ФКЗ, от 4.10.2022 № 5–ФКЗ, от 4.10.2022 № 6–ФКЗ, от 4.10.2022,№ 7–ФКЗ, от 4.10.2022 № 8–ФКЗ) // Собрание законодательства РФ. 2020. № 31. Ст. 4398.