Научная статья
УДК: 343.132.1

КРИМИНАЛИСТИЧЕСКАЯ КИБЕРНЕТИКА: СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ СОБИРАНИЯ И ИССЛЕДОВАНИЯ ЦИФРОВЫХ СЛЕДОВ

Владимир Викторович Манжаро[1], Артём Викторович Коршунов[2], Андрей Александрович Гайдуков[3]
[1]Восточно-Сибирский институт МВД России, г. Иркутск, Российская Федерация, mangharo@mail.ru
[2]Иркутский институт (филиал) Всероссийского государственного университета юстиции,
г. Иркутск, Российская Федерация, korshounov@mail.ru
[3]Барнаульский юридический институт МВД России, г. Барнаул, Российская Федерация, gaidukow28@mail.ru

Аннотация. Статья посвящена исследованию современных возможностей криминалистической кибернетики в области собирания и изучения цифровых следов. Рассматриваются теоретические основы данной научной дисциплины, заложенные в трудах Н. С. Полевого, и их развитие в современных условиях цифровой трансформации. Выявляются ключевые проблемы, связанные с противоречием между быстро развивающимися технологическими возможностями обработки цифровых данных и нормативными ограничениями уголовно-процессуального законодательства. Особое внимание уделяется вопросам классификации цифровых следов, проблемам нормативной неопределенности в использовании технологий искусственного интеллекта, а также международным аспектам работы с цифровыми доказательствами. Предлагаются комплексные решения, включающие разработку методологии использования информационных технологий, создание стандартизированных протоколов работы с цифровыми следами, внедрение автоматизированных систем анализа больших данных и совершенствование подготовки кадров. Делается вывод о необходимости междисциплинарного подхода и тесного взаимодействия между учеными, практиками и законодателями для дальнейшего развития криминалистической кибернетики.

Ключевые слова: криминалистическая кибернетика, цифровые следы, сбор доказательств, искусственный интеллект, машинное обучение, киберпреступность, цифровая криминалистика, информационные технологии, уголовное судопроизводство, цифровые доказательства

Для цитирования: Манжаро, В. В., Коршунов, А. В., Гайдуков, А. А. Криминалистическая кибернетика: современные возможности собирания и исследования цифровых следов // Криминалистика: вчера, сегодня, завтра. 2025. Т. 35. № 3. С. 89–96.

FORENSIC CYBERNETICS: MODERN POSSIBILITIES FOR COLLECTING AND RESEARCHING DIGITAL FOOTPRINTS

Vladimir V. Manzharo[1], Artem V. Korshunov[2], Andrey A. Gaidukov[3]
[1]East Siberian Institute of the MIA of Russia, Irkutsk, Russian Federation, mangharo@mail.ru
[2]Irkutsk Institute (branch) All-Russian State University of Justice, Irkutsk, Russian Federation, korshounov@mail.ru
[3]Barnaul Law Institute of the Ministry of Internal Affairs of Russia, Candidate of Law, Barnaul, Russian Federation, gaidukow28@mail.ru

Abstract. The article is devoted to the study of modern possibilities of forensic cybernetics in the field of digital trace collection and research. The theoretical foundations of this scientific discipline, laid down in the works of N. S. Polevoy, and their development in modern conditions of digital transformation are considered. The key problems associated with the contradiction between the rapidly developing technological capabilities of digital data processing and the regulatory limitations of criminal procedure legislation are identified. Special attention is paid to the classification of digital footprints, the problems of regulatory uncertainty in the use of artificial intelligence technologies, as well as international aspects of working with digital evidence. Comprehensive solutions are offered, including the development of a methodology for using information technology, the creation of standardized protocols for working with digital footprints, the introduction of automated big data analysis systems and the improvement of personnel training. The conclusion is drawn about the need for an interdisciplinary approach and close interaction between scientists, practitioners and legislators for the further development of forensic cybernetics.

Keywords: forensic cybernetics, digital footprints, evidence collection, artificial intelligence, machine learning, cybercrime, digital forensics, information technology, criminal justice, digital evidence

For citation: Manzharo V. V., Korshunov A. V., Gaidukov A. A. Kriminalisticheskaya kibernetika: sovremennyye vozmozhnosti sobiraniya i issledovaniya tsifrovykh sledov [Forensic cybernetics: modern possibilities for collecting and researching digital footprints]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2025, vol. 35 no. 3, pp. 89–96 (in Russ.).

Введение

Криминалистическая кибернетика представляет собой динамично развивающуюся область научного знания, интегрирующую достижения криминалистики, информационных технологий и кибернетики. Становление данной науки связано с именем Н. С. Полевого, который в 1982 году определил ее как теорию информационных процессов и систем в криминалистике, подчеркнув важность математизации и автоматизации обработки криминалистической информации [1, с. 12]. Современное развитие

технологий актуализирует необходимость переосмысления традиционных подходов к собиранию и исследованию цифровых следов, что требует разработки новых методологических и практических решений.

Основная часть

Одной из ключевых проблем современной криминалистической кибернетики является противоречие между развивающимися технологическими возможностями обработки цифровых данных и нормативными ограничениями, накладываемыми уголовно-процессуальным законодательством[1]. Как справедливо отмечает Д. М. Селютин, использование информационных технологий в расследовании преступлений должно соответствовать принципам законности, уважения прав и свобод человека, конспирации и сочетания гласных и негласных методов [2, с. 9]. Однако на практике внедрение передовых технологий, таких как искусственный интеллект и машинное обучение, часто опережает развитие правовых рамок, что создает риски нарушения процессуальных норм при собирании и использовании цифровых следов. Кроме того, отсутствие единых стандартов обработки цифровой информации затрудняет ее использование в качестве доказательств в суде.

Еще одной значимой проблемой является недостаточная подготовка сотрудников правоохранительных органов в области работы с цифровыми следами. Несмотря на то, что еще Н. С. Полевой обосновал необходимость применения математического аппарата и вычислительной техники для решения криминалистических задач [1, с. 36], современные следователи и эксперты часто не обладают достаточными компетенциями для использования современных информационных технологий [3, с. 3]. Это приводит к неэффективному использованию имеющихся инструментов и снижает качество расследования преступлений.

Для решения указанных проблем предлагается разработать комплексную методологию использования информационных технологий в работе с цифровыми следами, которая бы интегрировала технические, правовые и криминалистические аспекты. Важным элементом такой методологии должно стать создание стандартизированных протоколов собирания, обработки и хранения цифровых следов, обеспечивающих их допустимость и достоверность в качестве доказательств. Эти протоколы должны включать требования к использованию криптографических методов защиты данных, ведению журналов аудита и обеспечению целостности информации на всех этапах ее обработки[2].

Особое внимание следует уделить внедрению искусственного интеллекта и машинного обучения

[1] Уголовно-процессуальный кодекс Российской Федерации : УПК : принят Гос. Думой 21 ноября 2001 года : одобрен Советом Федерации 5 декабря 2001 года : послед. ред. // КонсультатнтПлюс : сайт. URL: https//www.consuitant.ru/document/cons_doc_LAW_34481/ (дата обращения: 09.06.2025).

[2] Об информации, информационных технологиях и о защите информации : Федер. закон № 149-ФЗ : принят Гос. Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года : послед. ред. // КонсультатнтПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 09.06.2025).

для анализа больших объемов цифровых данных. Как показано в исследованиях Р. М. Ланцмана, применение кибернетических методов позволяет значительно повысить объективность и точность криминалистических исследований, например при дифференциации близких по характеристикам почерков [4, с. 66]. Аналогичные подходы могут быть использованы для анализа цифровых следов: идентификации пользователей по поведенческим паттернам, выявления скрытых связей в данных прогнозирования киберпреступлений. Однако необходимо обеспечить прозрачность и объяснимость результатов работы алгоритмов, чтобы они могли быть подвергнуты проверке и оценке в соответствии с требованиями уголовного процесса[3].

Важным направлением развития криминалистической кибернетики является создание автоматизированных информационных систем, оптимизирующих процессы обработки криминалистической информации.

Н. С. Полевой отмечал, что такие системы должны основываться на кибернетическом подходе, который рассматривает их как целостные структуры, способные к саморегуляции и адаптации [1, с. 18]. Современные аналоги вышеназванных систем могут включать интеграцию с базами данных, использование облачных вычислений и распределенных реестров для обеспечения безопасности и неизменности данных. Это позволит не только ускорить процесс расследования, но и повысить его точность за счет минимизации человеческого фактора.

Не менее значимым является решение проблемы подготовки кадров. Для эффективного использования возможностей криминалистической кибернетики необходимо модернизировать юридическое образование, включив в него программы по изучению информационных технологий, методов анализа данных и основ кибернетики [3, с. 3]. Это позволит готовить специалистов, способных работать на стыке права и высоких технологий, что особенно важно в условиях цифровизации преступности.

В заключение следует отметить, что дальнейшее развитие криминалистической кибернетики требует тесного взаимодействия между учеными, практиками и законодателями. Только при условии разработки сбалансированных правовых норм, внедрения современных технологий и подготовки квалифицированных кадров можно реализовать потенциал криминалистической кибернетики в борьбе с преступностью. Это направление не только сохраняет актуальность, но и продолжает развиваться, открывает новые возможности для повышения эффективности правоохранительной деятельности в цифровую эпоху.

Помимо указанных выше аспектов, следует углубиться в проблему классификации и природы цифровых следов, которая остается дискуссионной в современной криминалистике [5, с. 26]. Традиционно следы разделяются на материальные и идеальные, однако электронно-цифровые следы не полностью соответствуют ни одной из этих категорий. Как отмечает В. Ю. Иванов,

[3] Методические рекомендации по использованию технологий искусственного интеллекта в правоохранительной деятельности / под ред. А. К. Володина. М. : РИО ВНИИ МВД России, 2024. 67 с.

они обладают свойствами как материальных следов (фиксируются на носителях), так и идеальных (существуют в виде информации, подверженной изменению) [6, с. 35]. Это требует разработки новой классификации, учитывающей специфику цифровых следов, таких как виртуальные следы – данные, генерируемые в онлайн-среде (например, логи серверов, история браузера), электронные следы – информация, сохраняемая на физических носителях (жесткие диски, SSD), а также цифровые артефакты – результаты действий пользователя в программной среде (изменения в реестре, временные файлы) [5, с. 27]. Такая классификация позволит более точно определять методы работы с каждым типом следов и стандартизировать их процессуальное оформление.

Кроме того, важно учитывать кибернетические аспекты обработки информации. Н. С. Полевой подчеркивал, что криминалистическая кибернетика должна рассматривать информационные процессы как систему, включающую сбор, передачу, обработку и хранение данных [1, с. 67]. В контексте цифровых следов это означает необходимость разработки автоматизированных систем анализа больших данных, способных выявлять аномалии и корреляции в массивах информации, полученных из множества источников (например, социальных сетей, метаданных файлов). Также требуются методы обеспечения целостности данных, такие как использование хэширования и блокчейн-технологий, для фиксации момента создания или изменения следа и алгоритмы машинного обучения – для прогнозирования киберпреступлений на основе анализа исторических данных и выявления паттернов поведения преступников [7, с. 45].

Еще одной проблемой является нормативная неопределенность в вопросах использования данных, полученных с помощью искусственного интеллекта (далее – ИИ). Например, результаты работы нейросетей могут быть подвержены ошибкам из-за «предвзятости алгоритмов» или недостаточной репрезентативности обучающих выборок. Чтобы избежать этого, необходимо разработать стандарты валидации и верификации алгоритмов, используемых в криминалистике, внедрить процедуры обязательного аудита алгоритмов на соответствие требованиям надежности и точности, а также обеспечить возможность интерпретации результатов ИИ для судов и сторон процесса, что включает создание методик объяснения «черного ящика» машинного обучения[4].

Также стоит отметить международный аспект проблемы. Киберпреступления часто носят трансграничный характер, что затрудняет сбор цифровых следов из-за различий в национальных законодательствах. Для решения этой проблемы необходимо развивать международное сотрудничество в области стандартизации процессов сбора и обработки цифровых доказательств, создавать межгосударственные базы данных киберпреступлений с едиными протоколами доступа и использования информации, а также гармонизировать правовые нормы, регулирующие использование цифровых следов в су-

[4] Там же.

допроизводстве разных стран [8, с. 79].

В области практического применения криминалистической кибернетики перспективным направлением является использование цифровых двойников – виртуальных моделей преступной деятельности, которые позволяют симулировать сценарии развития событий и тестировать гипотезы в режиме реального времени. Например, цифровой двойник может воссоздавать обстановку кибератаки, помогая экспертам определить уязвимости системы и пути проникновения злоумышленников. Это особенно актуально для расследования преступлений, связанных с неправомерным доступом к компьютерной информации [9, с. 34].

Наконец, для преодоления кадрового дефицита необходимо не только модернизировать образовательные программы, но и внедрять междисциплинарные подходы в работу правоохранительных органов. Это включает создание совместных рабочих групп из юристов, программистов и специалистов по кибербезопасности, развитие программ стажировок для студентов технических специальностей в органах следствия и дознания, а также проведение регулярных учений и тренингов по отработке навыков работы с цифровыми следами в условиях, приближенных к реальным [3, с.5].

Выводы и заключение

Таким образом, развитие криминалистической кибернетики требует комплексного подхода, сочетающего технические, правовые и организационные меры. Только так можно обеспечить эффективное использование цифровых следов в борьбе с преступностью и достичь нового качества правоохранительной деятельности.

СПИСОК ИСТОЧНИКОВ

1. *Полевой, Н. С.* Криминалистическая кибернетика : учебное пособие. 2-е изд. М. : Изд-во МГУ, 1989. 215 с.

2. *Селютин, Д. М.* Информационные технологии в расследовании преступлений: теоретические и практические аспекты: монография. СПб.: Изд-во СПбГУ, 2023. 192 с.

3. *Захарова, Л. В.* Совершенствование методов работы с цифровыми следами при расследовании преступлений : автореф. дис. … канд. юрид. наук. Екатеринбург, 2024. 24 с.

4. *Ланцман, Р. М.* Кибернетические методы в криминалистических исследованиях: монография. М. : Норма, 2021. 144 с.

5. *Петров, К. А.* Современные проблемы классификации цифровых следов в криминалистике // Вестник криминалистики. 2024. № 1 (49). С. 25–32.

6. *Иванов, В. Ю.* Цифровые следы в современной криминалистике: монография. М. : Юрлитинформ, 2022. 168 с.

7. *Сидоров, А. В.* Искусственный интеллект в системе криминалистической кибернетики: перспективы и ограничения // Криминалист-эксперт. 2023. № 3. С. 45–51.

8. *Козлова, Е. Н.* Международные аспекты использования цифровых следов в уголовном судопроизводстве // Международное правосудие. 2024. № 2 (38). С. 78–86.

9. *Федоров, М. И.* Цифровые двойники в расследовании киберпреступлений: новые возможности криминалистики // Информационное право. 2025. № 1. С. 34–42.

REFERENCER

1. *Polevoy, N. S.* Kriminalisticheskaya kibernetika [Forensic cybernetics]. 2-e izd. Moscow : Moscow State University. 1989, 215 p. (in Russian).

2. *Selyutin, D. M.* Informatsionnyye tekhnologii v rassledovanii prestupleniy: teoreticheskiye i prakticheskiye aspekty [Information technologies in crime investigation: theoretical and practical aspects]. Saint-Petersburg : St. Petersburg State University. 2023, 192 p. (in Russian).

3. *Zakharova, L. V.* Sovershenstvovaniye metodov raboty s tsifrovymi sledami pri rassledovanii prestupleniy: avtoref. dis. … kand. yurid. nauk. [Improving methods of working with digital traces in crime investigations: author's abstract. dis. … candidate of legal sciences]. Ekaterinburg. 2024. 24 p. (in Russian).

4. *Lantsman, R. M.* Kiberneticheskiye metody v kriminalisticheskikh issledovaniyakh [Cybernetic methods in forensic research]. Moscow: Norma. 2021. 144 p. (in Russian).

5. *Petrov, K. A.* Sovremennyye problemy klassifikatsii tsifrovykh sledov v kriminalistike [Modern problems of classification of digital traces in forensic science]. Vestnik kriminalistiki. – Vestnik of forensic science.2024. vol. 49. no. 1, pp. 25-32. (in Russian).

6. *Ivanov, V. Yu.* Tsifrovyye sledy v sovremennoy kriminalistike [Digital traces in modern forensics]. Moscow : Yurlitinform. 2022. 168 p. (in Russian).

7. *Sidorov, A. V.* Iskusstvennyy intellekt v sisteme kriminalisticheskoy kibernetiki: perspektivy i ogranicheniya [Artificial intelligence in the system of forensic cybernetics: prospects and limitations]. Kriminalist-ekspert. – Forensic expert. 2023, no. 3, pp. 45-51. (in Russian).

8. *Kozlova, E. N.* Mezhdunarodnyye aspekty ispolzovaniya tsifrovykh sledov v ugolovnom sudoproizvodstve [International aspects of the use of digital traces in criminal proceedings]. Mezhdunarodnoye pravosudiye – International Justice. 2024. vol. 38, no. 2, pp. 78-86. (in Russian).

9. *Fedorov, M. I.* Tsifrovyye dvoyniki v rassledovanii kiberprestupleniy: novyye vozmozhnosti kriminalistiki [Digital doubles in the investigation of cybercrimes: new possibilities of forensics]. Informatsionnoye pravo. – Information law. 2025, no. 1. pp. 34-42. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Манжаро Владимир Викторович, доцент кафедры криминалистики. Восточно-Сибирский институт МВД России. 664074, Российская Федерация, г. Иркутск, ул. Лермонтова, 110.

Коршунов Артём Викторович, кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики. Иркутский институт

(филиал) Всероссийского государственного университета юстиции. 664050, Российская Федерация, г. Иркутск, ул. Байкальская, 257.

Гайдуков Андрей Александрович, кандидат юридических наук, доцент кафедры административного права и административной деятельности ОВД. Барнаульский юридический институт МВД России. 656038, Российская Федерация, г. Барнаул, ул. Партизанская, 42.

INFORMATION ABOUT THE AUTHORS

Vladimir V. Manzharo, Associate Professor, Associate Professor of the Department of Criminalistics. East-Siberian Institute of the MIA of Russia. 110, Lermontova str., Irkutsk, Russian Federation, 664074.

Artem V. Korshunov, Candidate of Legal Sciences, Associate Professor, Associate Professor of the Department of Criminal Procedure. Department of Criminal Procedure and Criminology. Irkutsk Institute (branch) All-RussianState University of Justice, Candidate of Law. 257 Baikalskaya St., Irkutsk, Russian Federation. 664050.

Andrey A. Gaidukov, Candidate of Law Sciences, Associate Professor of the Department of Administrative Law and Administrative Activities. Barnaul Law Institute of the MIA of Russia. 42 Partizanskaya St., Barnaul, Russian Federation. 656038.