

Азиатско-Тихоокеанский регион: экономика, политика, право. 2024. Т. 26, № 3. С. 158–168.  
Pacific Rim: Economics, Politics, Law. 2024. Vol. 26, no. 3. P. 158–168.

Научная статья

УДК 343.982.352:004(470+571)

<https://doi.org/10.24866/1813-3274/2024-3/158-168>

## К вопросу применения цифровой криминалистики в современных условиях

Данила Дмитриевич Архипов<sup>1</sup>, Юлия Юрьевна Гарцева<sup>2</sup>✉,  
Виктор Юрьевич Миллер<sup>2</sup>

<sup>1</sup>Управление МВД России по Нижнему Новгороду,  
Нижний Новгород, Российская Федерация

<sup>2</sup>Нижегородская академия МВД России, Нижний Новгород, Российская Федерация  
✉ [yulya.gartseva@bk.ru](mailto:yulya.gartseva@bk.ru)

*Аннотация.* Цифровая криминалистика является одним из основных направлений криминалистики в XXI в., так как большинство преступлений совершается с помощью информационно-коммуникационной сети Интернет. В новом направлении криминалистики разрабатываются уникальные методы получения доказательств. Однако сегодня существуют и негативные моменты применения цифровой криминалистики, и связаны они могут быть с нехваткой специалистов и экспертов в данной области знаний.

*Ключевые слова:* цифровая криминалистика, специалисты, эксперты, криминалист, законодательство, цифровые права

*Для цитирования:* Архипов Д.Д., Гарцева Ю.Ю., Миллер В.Ю. К вопросу применения цифровой криминалистики в современных условиях // Азиатско-Тихоокеанский регион: экономика, политика, право. 2024. Т. 26, № 3. С. 158–168.

Original article

## On the issue of application of digital forensics in modern conditions

Danila D. Arkhipov<sup>1</sup>, Yulia Yu. Gartseva<sup>2</sup>✉, Viktor Yu. Miller<sup>2</sup>

<sup>1</sup>Department of the Ministry of Internal Affairs of Russia for the city of Nizhny Novgorod,  
Nizhny Novgorod, Russian Federation

<sup>2</sup>Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia,  
Nizhny Novgorod, Russian Federation

✉ [yulya.gartseva@bk.ru](mailto:yulya.gartseva@bk.ru)

© Архипов Д.Д., Гарцева Ю.Ю., Миллер В.Ю., 2024

*Abstract.* Digital criminology is one of the main areas of criminology in the era of the twenty-first century, since most crimes are committed using the Internet information and communication network. Unique methods of obtaining evidence are being developed in a new area of criminology. However, today there are also negative aspects of the use of digital forensics, and they may be related to the lack of specialists and experts in this field of knowledge.

*Keywords:* digital forensics, specialists, experts, criminologist, legislation, digital rights

*For citation:* Arkhipov D.D., Gartseva Yu.Yu., Miller V.Yu. On the issue of application of digital forensics in modern conditions. *PACIFIC RIM: Economics, Politics, Law*, 2024, vol. 26, no. 3, pp. 158–168. (In Russ.).

С приходом в нашу жизнь цифровых технологий, кроме положительных моментов в виде камер видеонаблюдения, электронных почтовых ящиков, электронных денежных средств, появились и новые нарушения прав человека, которые входят в состав преступлений и используются посредством цифровых технологий. Такие преступления могут быть квалифицированы в рамках статей: 146, 159–159<sup>6</sup>, 193<sup>1</sup>, 228<sup>1</sup>, 272–274<sup>1</sup> Уголовного кодекса Российской Федерации (УК РФ). Данный перечень статей имеет особую сложность с точки зрения квалификации и криминалистического изучения места преступления. Изучение цифровых следов является одним из новейших направлений правоприменителя: институты, предусмотренные статьями 138<sup>1</sup> и 159<sup>6</sup> УК РФ, всегда представляли интерес в деятельности силовых структур [1, с. 7–11], поскольку деятельность правоохранительных органов при выявлении и раскрытии преступлений нередко связана с применением технических средств, предназначенных для негласного получения информации. Значимость данных институтов значительно возросла с изменением общественно-политической обстановки в России. Стоит обратить внимание и на то, что экономические и политические кризисы в обществе всегда сопровождаются вооруженными конфликтами по социальным, этническим, национальным и религиозным мотивам.

Реформирование силовых структур, то есть повышение уровня их технической оснащенности, усиление их социальной защищенности, совершенствование профессиональной подготовки в области обеспечения государственной и общественной безопасности становится главным направлением политики Российской Федерации [2, с. 505–509].

Статистика говорит нам о стабильном приросте преступности с 2010 по 2015 г. По нашему мнению, это связано с реформированием системы МВД, так как в 2011 г. была проведена масштабная реформа перехода от милиции к полиции, и только в

2016 г. эта реформа была полностью реализована. Данный вывод сделан на основании графика, где показано, что именно в 2016 г. начался резкий спад преступности (рис. 1).

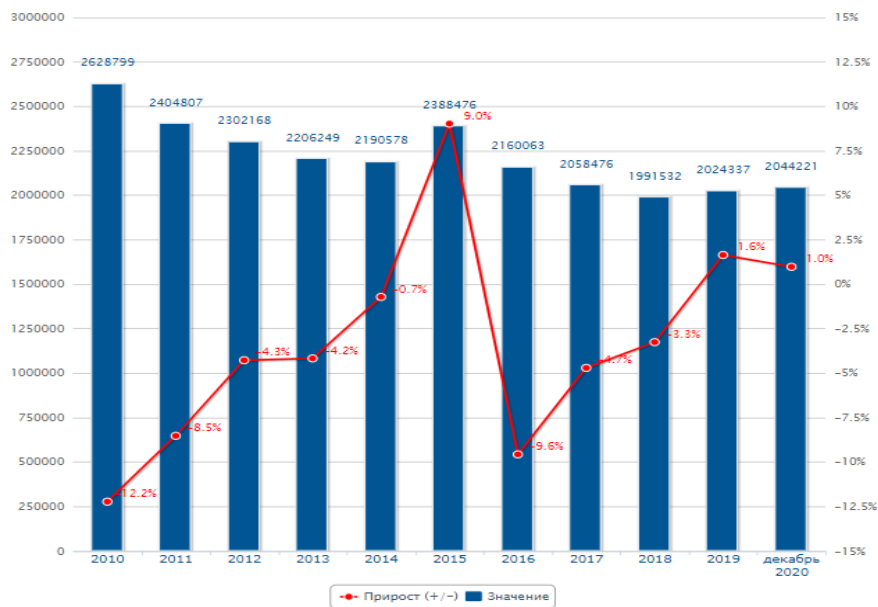


Рис. 1. Статистические данные за 10 лет [3]

Наблюдается также прирост преступности к декабрю 2020 г. На наш взгляд, это обусловлено, во-первых, эпидемиологической обстановкой распространения инфекции COVID-19, во-вторых, нехваткой кадровых ресурсов и, в-третьих, недостаточным уровнем подготовки из-за распространения инфекции COVID-19 [4, с. 108–114].

Создавшиеся условия открыли возможность для распространения цифровых преступлений. Вот почему мы считаем необходимым подробно исследовать такой узкий аспект теории и практики, как цифровая криминалистика.

Цифровая криминалистика приобретает особую актуальность в связи с внесением в 2019 г. изменений в положения Гражданского кодекса Российской Федерации (ГК РФ), а именно в статью 128, в которой появился новый термин «цифровые права», а также дополнением ГК РФ статьей 141.1 – цифровые права. Объектом цифровых прав может выступать цифровое имущество, не относящееся к материальным благам, то есть физически этой вещи не существуют, но за данные предметы цифрового мира платятся настоящие денежные средства. Примером таких прав является инвентарь в играх: игроки приобретают на цифровых платформах для своих персонажей предметы декора и т.д. Также цифровые права могут предусматривать цифровые активы, такие как токены, либо иные денежные средства в виде криптовалюты. Так, в мае 2018 г. постановлением Девятого арбитражного апелляционного суда по

делу №09АП-16416/18 криптовалюта впервые была признана на территории Российской Федерации в качестве имущества. В связи с изложенным стоит отметить, что введение в нормы ГК РФ понятия цифровых прав открыло возможности для совершения преступлений в сети Интернет.

С учетом приведенных нами изменений в законодательстве можно выделить следующие задачи цифровой криминалистики: интернет-розыск следов преступления; изучение историй использования браузеров; изъятие из телефона (иных технических устройств) истории использования данного технического устройства; отслеживание IP-адреса за определенный промежуток времени; изъятие с устройства удаленных переписок.

Есть гипотеза, что при совершении преступлений, связанных с кибернетикой, преступники оставляют цифровые следы: гражданство лица; расовую принадлежность; рост, вес, изображение лица; половую принадлежность; сексуальные предпочтения (если преступления связаны с составами, предусмотренными ст. 131–135 УК РФ); психологическое состояние лица; политическую и идеологическую принадлежность; финансовое положение лица.

В цифровой криминалистике выделяют два основных вида отпечатков:

- активные цифровые отпечатки: под данным термином понимают фактические следы преступления, то есть видеозапись, изображение, голос;
- пассивные цифровые отпечатки: под ним необходимо понимать те обстоятельства и доводы, которые косвенно относятся к данному лицу, то есть его увлечение, хобби, повседневная жизнедеятельность, мысли, изложенные в просторах сети Интернет, изучение им определенных вопросов в сети, взгляды и т. д. [5, с. 61–69].

На сегодняшний день принято выделять семь основных этапов цифровой криминалистики.

1. Идентификация – процесс выявления событий преступления в цифровых сетях (Интернет) и технических средствах.

2. Сохранение – деятельность, направленная на изъятие следов преступления из цифровых носителей уполномоченным лицом, имеющим определенные навыки и знания в данной области.

3. Сбор – процедура отбора прямых доказательств из сохраненных материалов, а также изучение косвенных следов преступления.

4. Исследование – процесс по изучению собранных данных и процедура извлечения скрытых данных в диалогах в социальных сетях и иных мессенджерах, пропуск информации через специализированные программы для подтверждения обвинения и доказательств по материалам дела.

5. Анализ – деятельность криминалиста по процессу ручной фильтрации и изучению полученных фактов и доказательств, то есть поиск мотивов пользования той

или иной программой, сайтом или социальной сетью, а также время использования и его продолжительность.

6. Представление – процедура отражения полученных цифровых улик, следов преступления в документации, то есть подготовка протокола с фототаблицей и разъяснение данных доводов.

7. Решение – деятельность криминалиста, связанная с подготовкой отчета и передачи следователю.

Также следует отметить, что институты, предусмотренные статьями 138<sup>1</sup> и 159<sup>6</sup> УК РФ, играют важную роль в деятельности правоохранительных органов. Результаты исследования позволяют сделать вывод о том, что вопрос неточности законодательной формулы является достаточно актуальной проблемой в уголовном праве при идентификации следов преступления.



Рис. 2. Следы преступных действий

На рис. 2 представлена таблица с видами следов, которые полиция может использовать в качестве доказательства. Но возникают сложности в поиске таких следов, поэтому мы предлагаем внедрять систему искусственного интеллекта в деятельность МВД, чтобы облегчить поиск следов преступления и их доказывание [6, с. 27–31].

Доказывание по уголовному делу в России при осуществлении уголовного преследования проводится при помощи тех доказательств, которые предусмотрены Уголовно-процессуальным кодексом Российской Федерации (УПК РФ). Наиболее значимыми являются «заключение эксперта» и «показания эксперта», они входят в число тех доказательств, которые прямо указаны в уголовно-процессуальном законодательстве. Стоит отметить, что круг доказательств, которые должны быть собраны и могут быть получены по конкретному уголовному делу, не является четко определенным и зафиксированным в каком-либо нормативно-правовом акте. В каждом конкретном случае определение качественного и количественного состава доказательств на стадии досудебного производства по уголовному делу производится лицом, осуществляющим предварительное следствие либо ведущим дознание. В ходе судебного рассмотрения уголовного дела вопрос о том, может ли доказательство быть принято для подтверждения тех или иных обстоятельств, решается судом. Иные участники уголовного судопроизводства вправе инициировать получение доказательства, в том числе путем его предоставления, но придание статуса доказательства осуществляется только следователем, дознавателем либо судом.

Преимущество цифровой криминалистики заключается в первую очередь в том, что цифровые следы возможно выявить даже со сломанного технического устройства. Данный вид криминалистики наиболее эффективный, так как большинство преступлений осуществляется с помощью информационно-коммуникационных средств, интернета, и в данной цифровой среде можно выявить множество цифровых улик и следов.

«Цифровой фасилитатор» способен являться результатом цифровой криминалистики. На сегодняшний день создано программное обеспечение, которое реорганизует 2D-фотографии в имитированные 3D-модели личности приблизительно за одну секунду, при этом пользователи программного обеспечения имеют все шансы менять состояние либо представление личности подозреваемого. Полученное изображение может быть проанализировано абсолютно всеми методами определения лиц как на компьютере, так и ином цифровом устройстве. Необходимо подчеркнуть, что развитие подобных алгоритмов дает возможность сотрудникам правоохранительных органов моментально распознавать обвиняемых.

Несмотря на то, что персональный компьютер способствует отбору следов, составляющих основу информации, для формирования схожести имеющейся информации были разработаны нейронные сети, представляющие собой специфический

метод машинного обучения, который отлично подходит для решения задач классификации и прогнозирования. Они являются полезным инструментом для работы с элементами, ориентированными на большие данные, представляющими интерес для правоохранительных органов. Модели нейронных сетей для прогнозирования конкретных видов преступлений с использованием информации о местоположении и времени разработаны для демонстрации применения их в своей деятельности органами внутренних дел. Модели прогнозирования преступности с использованием нейросетей используют геопространственность для предоставления немедленной информации о преступлениях в целях упрощения процесса принятия решений правоохранительными органами. Эти модели способны предсказывать тип совершаемого преступления в 16,4% случаев для 27 различных видов преступлений или в 27,1% случаев, когда аналогичные преступления группируются в семь категорий преступлений. Нейронные сети прогнозирования местоположения способны предсказывать местоположение почтового индекса или соседнего местоположения в 31,2% случаев.

NNS – это методология машинного обучения, которая отлично справляется с задачами классификации и прогнозирования. Поскольку NNS обучаются, они способны решать сколь угодно сложные задачи (Хорник, 1991). Нейронные сети широко применяются для решения проблем в различных областях, включая бизнес (Веллидо и др., 1999), инженерное дело (Bose, 1994), медицину (Вахт, 1991), естественные науки (Sundararaj и др., 1999), а в последнее время – и криминологию (Oatley и др., 2006).

NNS обучаются с помощью одного из двух механизмов - контролируемого обучения, для которого требуются исторические данные с известными результатами, и неконтролируемого обучения, которое извлекает закономерности непосредственно из данных. Оба метода требуют, чтобы NN был обучен. Существуют различные алгоритмы обучения для использования в каждом типе NN, причем обратное распространение наиболее популярно для обучения под наблюдением (Jayalakshmi and Santhakumaran, 2011), а самоорганизующиеся карты (SOM) наиболее приемлемы для обучения без присмотра (Oatley et al., 2006). Известны гибридные методы, сочетающие контролируемое и неконтролируемое обучение, такие как популярная сверхточная NN (CNN).

Все NN имеют входной уровень, который определяет переменные, предоставляемые NN для обучения, и выходной уровень, который определяет желаемое решение для классификации или прогнозирования. Контролируемое обучение и гибридные модели также содержат один или несколько скрытых уровней, каждый из которых полностью связан со следующим уровнем с помощью взвешенного соединения. Обучение происходит в этом типе NN путем определения ошибки тренировочного прогноза на основе фактического значения и распространения этой ошибки в обратном

направлении по сети для изменения весов соединений, чтобы лучше согласовать прогноз с правильным выходным значением. Пример архитектуры контролируемого обучения NN показан на рис. 3.

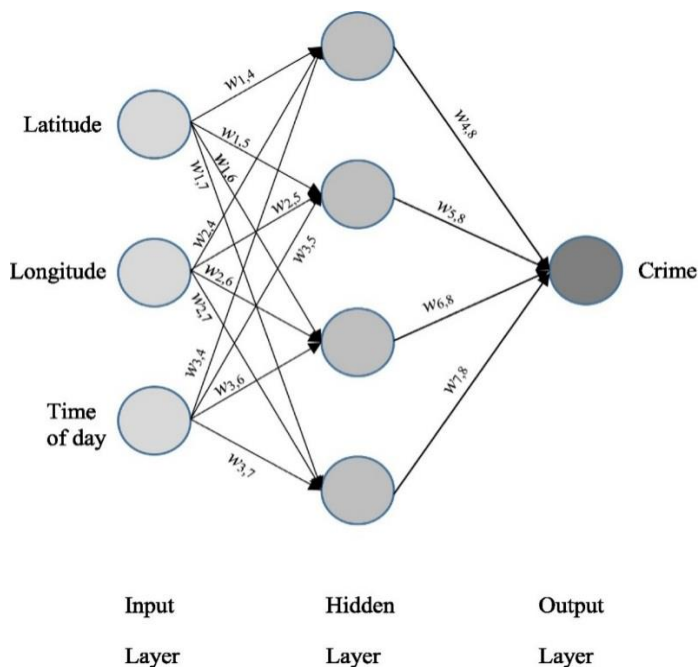


Рис. 3. Образец контролируемого обучения ANN [Многослойный перцептрон (MLP)] для прогнозирования типа преступления по данным о времени и месте

Валидация, или тестирование, моделей NN выполняется с данными, которые никогда не использовались при обучении оцениваемой модели. Это требуется для устранения неявной погрешности модели и имитации предполагаемого использования NN в реальном мире. Обычно доступные данные с известными результатами делятся на обучающий набор и набор для проверки, или тестирования, каждый из которых содержит уникальные примеры. Данные обучения также следует скорректировать, чтобы отразить сбалансированные пропорции прогнозируемых классов с целью помочь NN равномерно изучить все классы и не переучивать более распространенные классы (Weiland Dunbrack Jr, 2013).

С учетом изложенного следует отметить, что цифровые технологии в современном мире необходимы, особенно при выявлении преступлений в цифровой экосистеме, которая развивается и совершенствуется. Соответственно, преступный мир в этой области тоже не стоит на месте. Но чтобы понизить процент преступности в цифровом пространстве, нужно внедрять нейронные сети в системы государственного



управления, а также в оперативно-разыскные мероприятия, так как цифровые технологии помогут не только найти преступника, но и идентифицировать его с точки зрения криминалистики, а также собрать полный пакет доказательств виновности того или иного лица.

### Список источников

1. Архипов Д.Д. Проблемы законодательного регулирования криптовалюты // Международный форум молодых ученых: сборник статей Международной научно-практической конференции, Москва, 01–02 декабря 2021 года. М.: Академия управления Министерства внутренних дел Российской Федерации, 2021. С. 7–11.
2. Архипов Д.Д., Мазин О.А., Миллер В.Ю. Фальсификация документов // Административная деятельность органов внутренних дел в современных условиях, Нижний Новгород, 28 апреля 2022 года. Нтжний Новгород: Нижегородская Академия Министерства внутренних дел Российской Федерации, 2022. С. 505–509.
3. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2020 года // МВД.РФ. URL: <https://мвд.рф/reports/item/22678184/>.
4. Архипов Д.Д., Фадеева Я.А. Раскрытие отдельных видов преступлений // Наука и образование в контексте глобальной трансформации: сборник статей V Международной научно-практической конференции. Петрозаводск: Международный центр научного партнерства «Новая Наука», 2023. С. 108–114.
5. Плясов К.А. Теоретические основы формирования криминалистической характеристики преступлений в сфере внешне экономической деятельности // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2017. № 3 (82). С. 61–69.
6. Плясов К.А. Комплексная методика расследования преступлений в сфере внешнеэкономической деятельности и криминалистическая ситуалогия // Юристь-Правоведь. 2018. № 1 (84). С. 27–33.

### References

1. Arkhipov D.D. Problemy zakonodatel'nogo regulirovaniya kriptovalyuty [Problems of legislative regulation of cryptocurrencies]. In: *Mezhdunarodnyi forum molodykh uchenykh: sbornik statei Mezhdunarodnoi nauchno-prakticheskoi konferentsii, Moskva, 01–02 dekabrya 2021 goda* [International Forum of Young Scientists: Collection of articles of the International Scientific and Practical Conference, Moscow, December 01–02, 2021]. Moscow: Academy of Management of the Ministry of Internal Affairs of the Russian Federation, 2021, pp. 7–11. (In Russ.).
2. Arkhipov D.D., Mazin O.A., Miller V. Yu. Fal'sifikatsiya dokumentov [Falsification of documents]. In: *Administrativnaya deyatel'nost' organov vnutrennikh del v sovremennykh usloviyakh, Nizhnii Novgorod, 28 aprelya 2022 goda* [Administrative activity of internal affairs bodies in modern conditions, Nizhny Novgorod, April 28, 2022]. Nizhny

Novgorod: Novgorod Academy of the Ministry of Internal Affairs of the Russian Federation, 2022, pp. 505–509. (In Russ.).

3. A brief description of the state of crime in the Russian Federation for January–December 2020. *Ministry of Internal Affairs. RF*. URL: <https://мвд.рф/reports/item/22678184>. (In Russ.).

4. Arkhipov D.D., Fadeeva Ya.A. Raskrytie ot del'nykh vidov prestuplenii [Disclosure of certain types of crimes]. In: *Nauka i obrazovanie v kontekste global'noi transformatsii: sbornik statei V Mezhdunarodnoi nauchno-prakticheskoi konferentsii* [Science and education in the context of global transformation: Collection of articles of the V International scientific and practical conference]. Petrozavodsk: International Center for Scientific Partnership "New Science", 2023, pp. 108–114. (In Russ.).

5. Plyasov K.A. Teoreticheskie osnovy formirovaniya kriminalisticheskoi kharakteristiki prestuplenii v sfere vneshne ekonomicheskoi deyatelnosti [Theoretical foundations of the formation of criminalistic characteristics of crimes in the field of foreign economic activity]. *Vestnik Vostochno-Sibirskogo instituta Ministerstva vnutrennikh del Rossii*, 2017, no. 3 (82), pp. 61–69. (In Russ.).

6. Plyasov K.A. Kompleksnaya metodika rassledovaniya prestuplenii v sfere vneshneekonomicheskoi deyatelnosti i kriminalisticheskaya situatsiologiya [Complex methodology of investigation of crimes in the field of foreign economic activity and criminalistic situationology]. *Yurist"-Pravoved"*, 2018, no. 1 (84), pp. 27–31. (In Russ.).

### **Информация об авторах**

Д.Д. Архипов – полицейский Управления МВД России по Нижнему Новгороду, Нижний Новгород, Российская Федерация, [arkhipov\\_d.d@mail.ru](mailto:arkhipov_d.d@mail.ru)

Ю.Ю. Гарцева – старший преподаватель кафедры конституционного и международного права Нижегородской академии МВД России, кандидат юридических наук, Нижний Новгород, Российская Федерация, [yulya.gartseva@bk.ru](mailto:yulya.gartseva@bk.ru)

В.Ю. Миллер – старший преподаватель кафедры деятельности ОВД в особых условиях Нижегородской академии МВД России, кандидат юридических наук, Нижний Новгород, Российская Федерация, [millerviktor@mail.ru](mailto:millerviktor@mail.ru).

### **Information about the authors**

D.D. Arkhipov, Police Officer of the Department of the Ministry of Internal Affairs of Russia in Nizhny Novgorod, Nizhny Novgorod, Russian Federation, [arkhipov\\_d.d@mail.ru](mailto:arkhipov_d.d@mail.ru)

Y.Y. Gartseva, Senior Lecturer at the Department of Constitutional and International Law of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Candidate of Law, Nizhny Novgorod, Russian Federation, [yulya.gartseva@bk.ru](mailto:yulya.gartseva@bk.ru)

V.Y. Miller, Senior Lecturer at the Department of Internal Affairs in Special Conditions of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia Candidate of Law, Nizhny Novgorod, Russian Federation, millerviktor@mail.ru.

Статья поступила в редакцию / The article received 10.04.2024;  
одобрена после рецензирования / revised 13.08.2024;  
принята к публикации / accepted 03.09.2024.