

Научная статья

УДК 343.98(075.8)

EDN PCRWRC

DOI 10.17150/2500-4255.2024.18(4).390-397



КРИМИНАЛИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ ЦИФРОВЫХ ОТПЕЧАТКОВ КОМПЬЮТЕРНЫХ УСТРОЙСТВ

В.Б. Вехов¹, А.Б. Смушкин²¹ *Московский государственный технический университет имени Н.Э. Баумана**(национальный исследовательский университет), г. Москва, Российская Федерация*² *Саратовская государственная юридическая академия, г. Саратов, Российская Федерация*

Информация о статье

Дата поступления

9 августа 2024 г.

Дата принятия в печать

27 сентября 2024 г.

Дата онлайн-размещения

15 октября 2024 г.

Ключевые слова

Цифровые следы; цифровые отпечатки компьютерных устройств; цифровая криминалистика; цифровые доказательства; поведенческий цифровой отпечаток

Аннотация. В статье рассматриваются актуальные теоретические и прикладные проблемы, связанные с определением понятия и возможности использования цифровых отпечатков компьютерных устройств, которые образуются при подключении и работе этих устройств в информационно-телекоммуникационных сетях, в целях судопроизводства. С позиций цифровой криминалистики авторами излагаются основные цели идентификации компьютерных устройств по их цифровым отпечаткам на основе выделенных основных и частных признаков. Констатируется, что цифровой отпечаток компьютерного устройства (*Device Fingerprint*) представляет собой цифровой след, который сформирован в виде производного значения параметров, конфигурации программного и аппаратного обеспечения конкретного компьютерного устройства. Подделать цифровой отпечаток компьютерного устройства практически невозможно. Рассматриваются основные направления применения цифровых отпечатков компьютерных устройств. Анализируется перечень параметров, применяемых для идентификации цифрового устройства по его компьютерному отпечатку в российской и зарубежной практике. В российской правовой практике цифровой отпечаток формируется на основе идентификаторов аппаратной части компьютерного устройства, версии операционной системы, версии браузера и др. Авторы указывают на существование двух видов цифровых отпечатков: отпечаток браузера (помогает идентифицировать как стационарные компьютеры, так и мобильные устройства) и отпечаток мобильного устройства. Анализируются преимущества и недостатки активного и пассивного режимов снятия цифровых отпечатков компьютерных устройств. В связи со сложным механизмом формирования отпечатка рассматриваемого вида, обусловленного его уникальностью и частотой изменения характеристик, выделяются обстоятельства, которые должны быть учтены при его получении. Представлены методы, направленные на повышение эффективности этой деятельности и последующей идентификации конкретного компьютерного устройства по его цифровым следам, а также система криминалистических ситуаций применения цифрового отпечатка компьютерного устройства.

В завершение констатируется, что цифровые отпечатки компьютерных устройств имеют большой идентификационный потенциал, использование которого возможно не только в рамках антифрод-систем, но и при предотвращении и расследовании компьютерных инцидентов и киберпреступлений, деанонимизации пользователей, а также в целях защиты авторских прав и формирования целевой рекламы.

Original article

FORENSIC EXAMINATION OF DIGITAL FINGERPRINTS OF COMPUTER DEVICES

Vitalii B. Vekhov¹, Alexander B. Smushkin²¹ *Bauman Moscow State Technical University (National Research University), Moscow, the Russian Federation*² *Saratov State Law Academy, Saratov, the Russian Federation*

Article info

Received

2024 August 9

Accepted

2024 September 27

Abstract. The authors examine the theoretical and practical problems connected with determining the concept and the possibilities of using digital fingerprints of computer devices, found in the information-communication networks, in court proceedings. The authors present key goals of identifying computer devices by their digital fingerprints based on selected key and specific features from the standpoint of digital criminalistics. It is stated that a device fingerprint is a digital trace formed as an arbitrary value of parameters, the

Available online
2024 October 15

Keywords

Digital traces; digital devices' fingerprints; digital forensics; digital evidence; behavioral digital fingerprint

configurations of software and hardware of a specific computer device. It is virtually impossible to falsify a digital fingerprint. Key areas of using device fingerprints are examined. The list of parameters used for identifying a digital device by its computer fingerprint in Russian and foreign practice is analyzed. In Russian legal practice, a digital fingerprint is formed by the identifiers of the device's hardware, operation system's version, browser's version, and others. The authors point out that there are two types of device fingerprints: browser fingerprint (helps identify both desktop and mobile devices) and mobile device's fingerprint. Due to a complex formation mechanism of this type of fingerprints connected with its unique character and frequency of changes in its features, the authors describe the circumstances that should be taken into consideration when obtaining it. They present some methods for improving the effectiveness of this work and further identification of a specific device by its digital fingerprints, as well as a system of criminalistic situations of using device fingerprints.

In conclusion it is stated that device fingerprints have a considerable identification potential that could be used not only within the framework of anti-fraud systems, but also in preventing and investigating computer-related incidents and cybercrimes, user de-anonymization, as well as protection of copyright and development of targeted advertising.

В период активной цифровизации и цифровой трансформации всех сфер жизни объем цифровых устройств, находящихся в пользовании граждан и организаций, растет по экспоненте. При этом использование устройств оставляет в киберпространстве цифровые следы. Компьютерная информация, цифровые следы и электронные носители информации все чаще используются в качестве доказательств в судах всех уровней в рамках не только уголовного, но и арбитражного, гражданского и административного процессов.

В криминалистике понятие следа является одним из системообразующих, непосредственно влияющих на понятийный аппарат науки и ее систему, а также на отдельные частные теории.

Цифровой след — это любая криминалистически значимая компьютерная информация, т.е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (прим. 1 к ст. 272 УК РФ). Эти следы являются материальными невидимыми следами. Разработке вопросов понятия, возникновения и исследования цифровых следов уделяли внимание многие ученые [1–6].

В основе механизма образования следов рассматриваемой категории лежит специфическое электронно-цифровое отображение двух и более взаимодействующих между собой объективных форм существования компьютерной информации. Оно происходит в искусственно созданной среде — в канале связи, информационной системе, информационно-телекоммуникационной сети, памяти иных электронных носителей информации. В связи с этим качественные

характеристики отображения информации значительно зависят от особенностей данной среды, специально заложенных в нее разработчиками. Указанные факторы определяют объем получаемых криминалистически значимых признаков, которые в дальнейшем могут быть связаны с уголовно-релевантной информацией, содержащейся в формирующихся следах.

При формировании цифровых следов на материальном носителе фиксируются не сами свойства наблюдаемого физического процесса, например звука, динамического изображения и т.п., а всего лишь цифровые значения параметров формализованной математической модели, положенной в основу технического устройства регистрации его реального проявления [7, с. 269].

Зафиксированный на электронном носителе информации след представляет собой сложную информационную структуру, в которой наряду со значимой уголовно-релевантной информацией содержится значительный объем вспомогательных данных, отвечающих за целостность следа и возможность его восприятия с помощью соответствующих программно-технических средств.

Цифровые следы изучаются в рамках частной криминалистической теории о компьютерной информации и средствах ее обработки, получившей условное название «Цифровая криминалистика». В зарубежной криминалистике для ее обозначения используется понятие Digital forensic, от англ. Digital forensic science (цифровая судебная наука). В последние годы в ее структуре стало формироваться такое новое направление, как криминалистическое исследование цифровых отпечатков компьютерных устройств.

Цифровой отпечаток компьютерного устройства (*Device Fingerprint*) представляет собой цифровой след, который сформирован в виде производного значения параметров, конфигурации программного и аппаратного обеспечения конкретного компьютерного устройства [8, с. 292–304]. Этот отпечаток может использоваться для идентификации в следующих целях:

- выполнение мероприятий по противодействию осуществлению неправомерного совершения операций без согласия пользователя (владельца) компьютерного устройства, в том числе для расследования компьютерных инцидентов;

- выявление дорожек цифровых следов — система последовательно расположенных по времени и логически взаимосвязанных записей о прохождении компьютерной информации по линиям связи через коммутационное оборудование оператора (-ов) связи от компьютера правонарушителя до компьютера потерпевшего (их исследование осуществляется по методу «*Time Line*»);

- выявление устройств, использовавшихся для подготовки, совершения и сокрытия компьютерных атак на критическую информационную инфраструктуру, т.е. целенаправленного воздействия программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации (п. 4 ст. 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»¹);

- установление использования устройства законным пользователем (владельцем) с использованием поведенческого цифрового отпечатка;

- для идентификации пользователей Даркнет [9, с. 77].

Цифровой отпечаток компьютерного устройства является его уникальным идентификатором, который крайне сложно, если вообще возможно, подделать, который, кроме того, предоставляет большой объем информации о типе и параметрах устройства пользователя.

Использование цифровых отпечатков компьютерных устройств дает достаточно высокую

степень точности идентификации. По данным американских исследователей, анализ цифровых отпечатков беспроводных устройств, действующих в активном режиме, дает результативность порядка 99 %. Пассивный же режим устройств позволяет идентифицировать их с точностью до 94 % [10]. Устройства на основе технологии 5G идентифицируются с точностью 97 % [11]. Устройства Интернета вещей (*IoT*) могут быть идентифицированы с помощью разработанных нейронных сетей с точностью 95,8 % [12], а по некоторым данным, 98 % [13, с. 118].

Зарубежные авторы отмечают возможность использования для идентификации устройства как явных идентификационных признаков (адреса интернет-протокола / контроля доступа к СМИ) либо неявных идентификаторов (характеристики сетевого трафика и радиосигнала), так и неявных признаков, извлекаемых из трассировки сетевого трафика, включая сетевые пакеты, MAC-фреймы и радиосигналы [14]. Предлагается также использование радиочастотных цифровых отпечатков устройств 5G, возникающих из-за «несоответствий в производственных процессах передающих терминалов, терминалов основной полосы частот и других аналоговых устройств, а также влияния производственных допусков» [11].

В российской практике цифровой отпечаток компьютерного устройства формируется на основе комплексной автоматической регистрации и сохранения следующих параметров:

- идентификаторов аппаратной части компьютерного устройства;

- версии операционной системы (далее — ОС);

- версии браузера, под которым понимается программное обеспечение для просмотра веб-страниц. В настоящее время большинство браузеров имеет также функционал поисковой системы: информационной системы, осуществляющей по запросу пользователя поиск в сети Интернет информации определенного содержания и предоставляющая ему сведения об указателе страницы сайта в сети Интернет для доступа к запрашиваемой информации, расположенной на сайтах, принадлежащих иным лицам, за исключением информационных систем, используемых для осуществления государственных и муниципальных функций, оказания государственных и муниципальных услуг, а также для осуществления иных публичных полномочий, установленных федеральными

¹ О безопасности критической информационной инфраструктуры Российской Федерации : Федер. закон от 26 июля 2017 г. № 187-ФЗ : (в ред. от 10 июля 2023 г.) // Собрание законодательства РФ. 2017. № 31, ч. 1. Ст. 4736.

законами (п. 20 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации»²);

– иных системных и аппаратных параметров устройства.

Как показывает практика, основная сложность в формировании отпечатка рассматриваемого вида состоит в определении баланса между его уникальностью и частотой изменения характеристик, которые применяются для его получения. При этом индивидуальны и неповторимы могут быть как сами признаки, используемые при идентификации устройства, так и совокупность стандартных признаков (идентификационная совокупность). Все эти признаки должны изучаться в комбинации и взаимосвязи.

Организациям, использующим цифровые отпечатки в своих технологических процессах, следует сохранять как первоначальный цифровой отпечаток устройства, так и изменения цифрового отпечатка в динамике с фиксацией времени получения этих отпечатков, поскольку на устройствах может происходить эволюция цифровых отпечатков — меняться или обновляться программное обеспечение либо проводиться апгрейд устройства, изменяя цифровой отпечаток. Данный метод позволяет проводить более точный их криминалистический анализ при совершении компьютерного инцидента и компьютерной атаки.

Выделяются два основных вида цифровых отпечатков компьютерных устройств: отпечаток браузера (помогает идентифицировать как стационарные компьютеры, так и мобильные устройства) и отпечаток мобильного устройства.

Снятие цифровых отпечатков возможно как в пассивном, так и в активном режимах. Пассивный режим позволит сохранить фактор неожиданности, поскольку считываются параметры, которые само устройство передает при подключении. Активный режим позволяет выделить большее количество параметров, но связан с направлением запросов на устройство пользователя (например, отпечатки *Audiocontext Data* и *Canvas Data*, непосредственно связаны с выполнением устройством пользователя действий по запросу проверяющей системы). На считывание некоторых параметров в таком режиме может потребоваться согласие пользователя.

² Об информации, информационных технологиях и о защите информации : Федер. закон от 27 июля 2006 г. № 149-ФЗ : (в ред. от 22 июня 2024 г.). // Собрание законодательства РФ. 2006. № 31, ч. 1. Ст. 3448.

При определении параметров, которые необходимо получать для формирования цифрового отпечатка, должны быть учтены следующие обстоятельства.

1. Устройства на базе операционной системы *Android* имеют более широкую совокупность общих и частных идентификационных признаков чем устройства с ОС *iOS*, поскольку в последнем максимально унифицированы свойства в рамках одного модельного ряда, и признаков, отвечающих критерию самостоятельности и малой частоты встречаемости (т.е. тех, которые могут использоваться в качестве идентификационных), крайне мало. Кроме того, устройства на базе ОС *Android* позволяют подготавливать пользовательские сборки программ.

2. Указанное обстоятельство требует перманентной разработки методов получения цифрового отпечатка у устройств с ОС *Android* и более редкой для устройств фирмы *Apple*.

3. Возможность получения цифрового отпечатка не абсолютна. В некоторых случаях могут быть получены нулевые (пустые) значения либо получение параметров ставится в зависимость от подтверждения запроса (предоставления разрешения) пользователем, что не всегда возможно. Также следует учитывать возможность эмуляции или прямой подделки запрашиваемых параметров пользователем (при этом изменение некоторых параметров устройства все-таки требует нижеуровневого доступа, снятия программных ограничений и прав администратора или супер-пользователя).

4. К изменению параметров компьютерного устройства могут привести, например, обновление системы, смена используемого браузера, переустановка мобильного приложения, установка плагинов, перезагрузка устройства, сброс установленных настроек устройства, обновление его программного обеспечения или даже шрифтов, смена SIM-карты (модуля идентификации мобильного абонента), замена комплектующих устройств.

5. Идентификационная совокупность, используемая в качестве цифрового отпечатка, может претерпевать эволюцию, меняться со временем. В этой связи в целях применения технологии цифрового отпечатка необходимо осуществлять сбор параметров, которые отвечают следующим условиям:

– извлечение параметров не должно создавать больших сложностей;

– для идентификации используются наиболее стабильные, сложные для изменения их значений пользователем, параметры;

– параметры, используемые для формирования цифровых отпечатков, должны отвечать критериям малой частоты встречаемости и уникальности для конкретного устройства.

Зарубежные авторы предлагают следующие требования, которым должен удовлетворять признак для формирования цифрового отпечатка компьютерного устройства: уникальность, стабильность, масштабируемость, разнообразие, эффективность, надежность, безопасность [15].

Наиболее подробно рассмотрен *алгоритм формирования цифрового отпечатка компьютерного устройства* в Стандарте Банка России СТО БР БФБО-1.7-2023 «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств»:

1. Приложение или веб-сайт проводит автоматический сбор множества данных с устройства пользователя на предмет общих, особых и уникальных параметров и настроек, а также сведений о конфигурации аппаратного обеспечения.

При этом идентификационные признаки для браузера (при производстве операции с компьютера) или мобильного устройства (смартфона, планшетного компьютера и т.д.) будут различными. С мобильных устройств снимается до 22 различных параметров, от MAC-адреса Bluetooth или WiFi-устройства, до массива имен шрифтов.

2. Зарегистрированная идентификационная информация о компьютерном устройстве объединяется в одну строку в заданном порядке в формате JSON, которая сохраняется отдельно в неизменном виде.

3. Строка с данной информацией передается в организацию для последующего вычисления функции хэширования (с длиной хэш-кода 512 бит) и применения полученного результата в качестве цифрового отпечатка компьютерного устройства. Фактически набор параметров устройства преобразовывается в строку фиксированной длины, состоящую из цифр и букв, которая непосредственно и используется в качестве цифрового отпечатка устройства для сопоставления с другими вычисленными функциями хэширования и определения их различия или идентичности³.

³ Стандарт Банка России СТО БР БФБО-1.7-2023. Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с

Даже если изолированно данные признаки не способны дать исследователям возможность точной идентификации устройства, то будучи объединенными, они обладают бесценными идентификационными свойствами, которые позволяют однозначно определить тип устройства и связать его с пользователем [16, с. 1322].

Первичный цифровой отпечаток вносится в базу эталонных цифровых отпечатков компьютерных устройств пользователя (владельца) для их последующей идентификации. Так как пользователь (владелец) может использовать несколько компьютерных устройств для дистанционного доступа к информационным ресурсам организации, эта база данных дополняется эталонными цифровыми отпечатками других компьютерных устройств, зарегистрированных на одного пользователя. При этом, как отмечается в зарубежных публикациях, точность идентификации может быть повышена за счет совместного использования методов классификации и вероятностно-статистического подхода [17, с. 582].

Кроме непосредственного отпечатка компьютерных устройств возможна также идентификация поведенческого цифрового отпечатка. Как верно отмечает Стив Голд (*Stive Gold*), истоки цифровой дактилоскопии как науки на самом деле восходят к началу Второй мировой войны, когда в 1939 г. офицеры британской разведки регулярно прослушивали немецкие радиотелеграфные передачи, добросовестно записывая все точки и тире азбуки Морзе. В 1980 г. корпорация *Rand* воспользовалась идеей для анализа времени между нажатием клавиш [18, с. 16]. В дальнейшем эти разработки получили развитие в направлении клавиатурного почерка и анализа движения мыши [19]. В настоящее время для составления поведенческого цифрового отпечатка возможно использование следующих параметров — голоса, динамики нажатия клавиш, взаимодействия с мышью или сенсорным экраном, динамики движений (фиксируемой с помощью акселерометра), поведенческому профилю и др. [20].

Типичные ситуации криминалистического применения цифрового отпечатка:

1. Сопоставление устройства, с которого производится операция с устройством, отпечаток

использованием технологии цифровых отпечатков устройств: принят и введен в действие приказом Банка России от 1 марта 2023 г. № ОД-335 «О введении в действие стандарта Банка России СТО БР БФБО-1.7-2023. URL: <https://cbr.ru/Crosscut/LawActs/File/6177> (дата обращения: 20.07.2024).

которого сохранен в базе данных эталонных цифровых отпечатков. При совпадении хэш-функций или различии параметров, из которых состоит хэш-функция, не более чем на 15 %⁴, делается вывод об идентичности устройств или использовании доверенного устройства прошедшего обоснованную эволюцию цифрового отпечатка. При превышении различия параметров делается предположение о попытке неправомерных действий.

2. При реализации мероприятий по проверке наличия волеизъявления пользователя на операцию:

- при расследования компьютерных инцидентов;
- при осуществлении операций, направленных на совершение финансовых сделок с использованием финансовой платформы.

В этих случаях используется также и поведенческий цифровой отпечаток.

3. В рамках выполнения следующих требований, приведенных в Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации»:

- информирования о компьютерных инцидентах федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также Центрального банка Российской Федерации в установленном порядке;

- при реагировании на компьютерные инциденты в порядке, утвержденном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации⁵.

⁴ Пункт 5.4.1 стандарта Банка России СТО БР БФБО-1.7-2023 «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств».

⁵ О безопасности критической информационной инфраструктуры Российской Федерации : Федер. закон от 26 июля 2017 № 187-ФЗ : (ред. от 10 июля 2023 г.) // Собрание законодательства РФ 2017. № 31, ч. 1. Ст. 4736.

4. В целях уголовного судопроизводства цифровые отпечатки компьютерных устройств могут быть получены:

- при производстве оперативно-розыскного мероприятия «Получение компьютерной информации» (п. 15 ст. 6 Федерального закона «Об оперативно-розыскной деятельности»⁶);

- по запросу прокурора, руководителя следственного органа, следователя, органа дознания и дознавателя (ч. 4 ст. 21 УПК РФ), который обязателен для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами;

- при производстве процессуальных, в том числе следственных, действий, например регламентированных ст. 176, 182, 183 и 186.1 УПК РФ.

5. Цифровые отпечатки компьютерных устройств, совместно с поведенческими цифровыми отпечатками, могут быть использованы в рамках построения цифрового профиля лица, разработки которого предлагаются многими учеными [21].

Таким образом, использование цифровых отпечатков компьютерных устройств имеет большой идентификационный потенциал, использование которого возможно не только в рамках антифрод-систем, но и при предотвращении и расследовании компьютерных инцидентов и киберпреступлений, деанонимизации пользователей, а также в целях защиты авторских прав и формирования целевой рекламы. Если фальсифицировать отдельные цифровые следы или удалить их (например, файлы *cookies*) еще возможно, то эмулировать или фальсифицировать всю идентификационную совокупность, используемую для цифрового отпечатка компьютерного устройства, а также поведенческого цифрового отпечатка его пользователя нереально. С учетом активного развития интеллектуальных систем представляется необходимым рекомендовать активизацию использования нейросетей и систем на основе искусственного интеллекта для формирования и идентификации цифровых отпечатков и аутентификации их пользователей.

⁶ Об оперативно-розыскной деятельности : Федер. закон от 12.08.1995 г. № 144-ФЗ // Собрание законодательства РФ. 1995. № 33. Ст. 3349.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Мещеряков В.А. Теоретические основы механизма слеодообразования в цифровой криминалистике : монография / В.А. Мещеряков. — Москва : Проспект, 2022. — 176 с. — EDN EJFPKB.

2. Агibalов В.Ю. Виртуальные следы в криминалистике и уголовном процессе : монография / В.Ю. Агibalов. — Москва : Юрлитинформ, 2012. — 152 с. — EDN SYPZGV.
3. Нестеров А.В. Виртуальные следы в криминалистике : учебник / А.В. Нестеров. — Москва : КноРус, 2024. — 153 с.
4. Теория информационно-компьютерного обеспечения криминалистической деятельности / Е.Р. Россинская, А.И. Семикаленова, И.А. Рядовский, Т.А. Сааков ; под ред. Е.Р. Россинской. — Москва : Проспект, 2022. — 256 с. — EDN CNRUBZR.
5. Цифровые следы преступлений : монография / А.М. Багмет, В.В. Бычков, С.Ю. Скобелин, Н.Н. Ильин. — Москва : Проспект, 2021. — 168 с. — EDN RJXQWJ.
6. Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности : автореф. дис. ... канд. юрид. наук : 12.00.09 / Н.Н. Лыткин. — Москва, 2007. — 24 с.
7. Мещеряков В.А. Следы преступлений в сфере высоких технологий / В.А. Мещеряков. — EDN RDFWJD // Библиотека криминалиста. — 2013. — № 5. — С. 265–270.
8. Цифровая криминалистика : учебник / под ред. В.Б. Вехова, С.В. Зуева. — 2-е изд., перераб. и доп. — Москва : Юрайт, 2024. — 490 с.
9. Боровик П.Л. Программно-техническое обеспечение установления сведений о лицах, совершающих преступления в скрытом сегменте сети интернет (DarkNet) / П.Л. Боровик. — EDN PQDKIA // Криминалистика — прошлое, настоящее, будущее: достижение и перспективы развития : материалы Междунар. науч.-практ. конф., Москва, 17 окт. 2019 г. / под общ. ред. А.М. Багмета. — Москва, 2019. — С. 75–77.
10. Ensuring the Longevity of WirelessHART Devices in Industrial Automation and Control Systems Using Distinct Native Attribute Fingerprinting / M.J. Maier, H.S. Hayden, M.A. Temple, M.C. Fickus // International Journal of Critical Infrastructure Protection. — 2023. — Vol. 43. — P. 100641.
11. Device Authentication for 5G Terminals via Radio Frequency Fingerprints / Ping Dong, Namin Hou, Yuting Tang [et al.] // High-Confidence Computing. — 2024. — P. 100222.
12. Fingerprinting Industrial IoT Devices Based on Multi-Branch Neural Network / Kai Yang, Qiang Li, Haining Wang [et al.] // Expert Systems with Applications. — 2024. — Vol. 238. — P. 122371.
13. Wi-Fi Device Identification Based on Multi-Domain Physical Layer Fingerprint / Jinghui Zhang, Zhengjia Xu, Junhe Li [et al.] // Computer Communications. — 2023. — Vol. 204. — P. 118–129.
14. Chowdhury R.R. A Survey on Device Fingerprinting Approach for Resource-Constraint IoT devices: Comparative Study and Research Challenges / R.R. Chowdhury, Pg E. Abas // Internet of Things. — 2022. — Vol. 20. — P. 100632.
15. A methodology to Identify Identical Single-Board Computers Based on Hardware Behavior Fingerprinting / P.M. Sánchez, J.M. Jorquera Valero, A.H. Celdrán [et al.] // Journal of Network and Computer Applications. — 2023. — Vol. 212. — P. 103579.
16. Kobusińska A. Big Data Fingerprinting Information Analytics for Sustainability / A. Kobusińska, K. Pawluczuk, J. Brzeziński // Future Generation Computer Systems. — 2018. — Vol. 86. — P. 1321–1337.
17. Salomatin A.A. Web User Identification Based on Browser Fingerprints Using Machine Learning Methods / A.A. Salomatin, A.Y. Iskhakov, A.O. Iskhakova // IFAC-PapersOnLine. — 2021. — Vol. 54, Iss. 13. — P. 582–587.
18. Gold S. Understanding the Digital Fingerprint / S. Gold // Network Security. — 2013. — Iss. 12. — P. 15–18.
19. Adeyemi R.I. Digital Behavioral-Fingerprint for User Attribution in Digital Forensics: Are we There Yet? / R. Adeyemi, S.V. Hein // Digital Investigation. — 2019. — Vol. 30. — P. 73–89.
20. Осин А.В. Обзор методов идентификации пользователя на основе цифровых отпечатков / А.В. Осин, Ю.В. Мурашко. — DOI 10.31854/1813-324X-2023-9-5-91-111 // Труды учебных заведений связи. — 2023. — Т. 9, № 5. — С. 91–111.
21. Зайцев О.А. Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений / О.А. Зайцев, П.С. Пастухов. — DOI 10.17072/1995-4190-2022-56-281-309. — EDN TBDSEX // Вестник Пермского университета. Юридические науки. — 2022. — № 56. — С. 281–308.

REFERENCES

1. Meshcheryakov V.A. *The Theoretical Basis of the Trace-formation Mechanism in Digital Criminalistics*. Moscow, Prospekt Publ., 2022. 176 p. EDN: EJFPKB.
2. Agibalov V.Yu. *Virtual Traces in Criminalistics and Criminal Process*. Moscow, Yurlitinform Publ., 2012. 152 p. EDN: SYPZGV.
3. Nesterov A.V. *Virtual Traces in Criminalistics*. Moscow, KnoRuc Publ., 2024. 153 p.
4. Rossinskaya E.R., Semikalenova A.I., Ryadovskii I.A., Saakov T.A.; Rossinskaya E.R. (ed.). *The Theory of Information-computer Support of Criminalistic Work*. Moscow, Prospekt Publ., 2022. 256 p. EDN: CNRUBZ.
5. Bagmet A.M., Bychkov V.V., Skobelin S.Yu., Il'in N.N. *Digital Traces of Crimes*. Moscow, Prospekt Publ., 2021. 168 p. EDN: RJXQWJ.
6. Lytkin N.N. *The Use of Computer-technical Traces in Investigating Property Crimes*. Cand. Diss. Thesis. Moscow, 2007. 24 p.
7. Meshcheryakov V.A. Traces of Crime in the Field of High Technologies. *Biblioteka kriminalista = Library of a Criminalist*, 2013, no. 5, pp. 265–270. (In Russian). EDN: RDFWJD.
8. Vekhov V.B., Zuev S.V. (ed.). *Digital Criminalistics*. 2nd ed. Moscow, Yurait Publ., 2024. 490 p.
9. Borovik P.L. Software-technical Support of Finding Information on Person Committing Crimes in the Hidden Part of the Internet (DarkNet). In Bagmet A.M. (ed.). *Criminalistics — Past, Present, Future: Achievement and Development Prospects. Materials of International Scientific Conference, Moscow, October 17, 2019*. Moscow, 2019, pp. 75–77. (In Russian). EDN: PQDKIA.
10. Maier M.J., Hayden H.S., Temple M.A., Fickus M.C. Ensuring the Longevity of Wireless HART Devices in Industrial Automation and Control Systems Using Distinct Native Attribute Fingerprinting. *International Journal of Critical Infrastructure Protection*, 2023, vol. 43, pp. 100641.
11. Ping Dong, Namin Hou, Yuting Tang, Yushi Cheng, Xiaoyu Ji, Device Authentication for 5G Terminals via Radio Frequency Fingerprints. *High-Confidence Computing*, 2024, pp. 100222.
12. Kai Yang, Qiang Li, Haining Wang, Limin Sun, Jiqiang Liu. Fingerprinting Industrial IoT Devices Based on Multi-Branch Neural Network. *Expert Systems with Applications*, 2024, vol. 238, pp. 122371.

13. Jinghui Zhang, Zhengjia Xu, Junhe Li, Qiangsheng Dai, Zhen Ling, Ming Yang. Wi-Fi Device Identification Based on Multi-Domain Physical Layer Fingerprint. *Computer Communications*, 2023, vol. 204, pp. 118–129.
14. Chowdhury R.R., Abas Pg E. A Survey on Device Fingerprinting Approach for Resource-Constraint IoT devices: Comparative Study and Research Challenges. *Internet of Things*, 2022, vol. 20, pp. 100632.
15. Sánchez P.M., Valero J.M.J., Celdrán A.H., Bovet G., Pérez M.G., Pérez G.M. A Methodology to Identify Identical Single-Board Computers Based on Hardware Behavior Fingerprinting. *Journal of Network and Computer Applications*, 2023, vol. 212, pp. 103579.
16. Kobusińska A., Pawluczuk K., Brzeziński J. Big Data Fingerprinting Information Analytics for Sustainability. *Future Generation Computer Systems*, 2018, vol. 86, pp. 1321–1337.
17. Salomatin A.A., Iskhakov A.Y., Iskhakova A.O. Web User Identification Based on Browser Fingerprints Using Machine Learning Methods. *IFAC-PapersOnLine*, 2021, vol. 54, iss. 13, pp. 582–587.
18. Gold S. Understanding the Digital Fingerprint. *Network Security*, 2013, iss. 12, pp. 15–18.
19. Adeyemi R.I., Hein S.V. Digital Behavioral-Fingerprint for User Attribution in Digital Forensics: Are we There Yet? *Digital Investigation*, 2019, vol. 30, pp. 73–89.
20. Osin A.V., Murashko Yu.V. Review of User Identification Methods Based on Digital Fingerprint. *Proceedings of Telecommunication Universities*, 2023, vol. 9, no. 5, pp. 91–111. (In Russian). DOI: 10.31854/1813-324X-2023-9-5-91-111.
21. Zaytsev O.A., Pastukhov P.S. Digital Personal Profile as an Element of the Information and Technological Strategy of Crime Investigation. *Vestnik Permskogo universiteta. Yuridicheskie nauki = Perm University Herald. Juridical Sciences*, 2022, no. 56, pp. 281–308. (In Russian). EDN: TBDSEX. DOI: 10.17072/1995-4190-2022-56-281-309.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Вехов Виталий Борисович — профессор кафедры безопасности в цифровом мире Московского государственного технического университета имени Н.Э. Баумана (национального исследовательского университета), доктор юридических наук, профессор, академик, заслуженный деятель науки и образования Российской академии естественных наук, г. Москва, Российская Федерация; e-mail: vbvehov@bmstu.ru.

Смушкин Александр Борисович — доцент кафедры криминалистики Саратовской государственной юридической академии, кандидат юридических наук, доцент, г. Саратов, Российская Федерация; e-mail: Skif32@yandex.ru.

ВКЛАД АВТОРОВ

Все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

ДЛЯ ЦИТИРОВАНИЯ

Вехов В.Б. Криминалистическое исследование цифровых отпечатков компьютерных устройств / В.Б. Вехов, А.Б. Смушкин. — DOI 10.17150/2500-4255.2024.18(4).390-397. — EDN PCRWRC // Всероссийский криминологический журнал. — 2024. — Т. 18, № 4. — С. 390–397.

INFORMATION ABOUT THE AUTHORS

Vekhov, Vitalii B. — Professor, Department of Security in the Digital World, Bauman Moscow State Technical University (National Research University), Doctor of Law, Professor, Academician, Honored Worker of Science and Education of the Russian Academy of Natural Sciences, Moscow, the Russian Federation; e-mail: vbvehov@bmstu.ru.

Smushkin, Alexander B. — Ass. Professor, Department of Criminalistics, Saratov State Law Academy, Ph.D. in Law, Saratov, the Russian Federation; e-mail: Skif32@yandex.ru.

CONTRIBUTION OF THE AUTHORS

The authors contributed equally to this article. The authors declare no conflicts of interests.

FOR CITATION

Vekhov V.B., Smushkin A.B. Forensic Examination of Digital Fingerprints of Computer Devices. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2024, vol. 18, no. 4, pp. 390–397. (In Russian). EDN: PCRWRC. DOI: 10.17150/2500-4255.2024.18(4).390-397.