Научная статья
УДК 348.98
DOI: 10.18384/2949-513X-2025-1-94-102

«ГОРЯЧИЕ» ЭЛЕКТРОННЫЕ ЦИФРОВЫЕ СЛЕДЫ

Смушкин А. Б.
Саратовская государственная юридическая академия, г. Саратов, Российская Федерация
e-mail: skif32@yandex.ru; ORCID: 0000-0003-1619-8325

Поступила в редакцию 14.02.2025
После доработки 12.03.2025
Принята к публикации 24.03.2025

Аннотация
Цель. Выявить группы электронных цифровых следов, подлежащих безотлагательному выявлению и исследованию.
Процедура и методы. В работе использованы материалистическая диалектика как всеобщий метод, а также общенаучные методы – анализа, синтеза, моделирования, экстраполяции и др.
Результаты. Определена группа следов в киберпространстве, которой предлагается присвоить условное наименование «горячие электронные цифровые следы», предложена авторская трактовка данной категории. В ходе анализа указанного вида следов предложена авторская дифференциация их на волатильные и актуальные.
Теоретическая и/или практическая значимость. Введена авторская трактовка «горячих цифровых следов», что имеет большое теоретическое значение для цифровой криминалистики. Подробно рассмотренные отдельные виды волатильных и актуальных следов с практической точки зрения способствуют более точному направлению работы следователей и специалистов, сохранению максимального доказательного потенциала обнаруженных объектов.

Ключевые слова: актуальные следы, виртуальные следы, волатильные следы, горячие следы, расследование по горячим следам, следы в киберпространстве, электронные цифровые следы

Благодарности. Исследование выполнено за счёт гранта Российского научного фонда № 24-28-00312.

Для цитирования:
Смушкин А. Б. «Горячие» электронные цифровые следы // Московский юридический журнал. 2025. № 1. С. 94–102. https://doi.org/10.18384/2949-513X-2025-1-94-102.

Original research article

DIGITAL FOOTPRINTS NOTICED “HOT ON THE HEELS”

A. Smushkin
Saratov State Law Academy, Saratov, Russian Federation
e-mail: skif32@yandex.ru; ORCID: 0000-0003-1619-8325

Received by the editorial office 14.02.2025
Revised by the author 12.03.2025
Accepted for publication 24.03.2025

Abstract
Aim. To identify groups of electronic digital footprints to be immediately identified and investigated**.**

Methodology. The main method of scientific research was formal-legal, with the help of which the provisions of existing legal acts in the field of consolidation and implementation of reproductive human rights, as well as judicial practice of their application, were analyzed. General scientific methods, such as analysis, generalization, logical method, etc., were also used.
Results. A group of traces in cyberspace has been identified, which is proposed to be given the conditional name "digital footprints noticed "hot on the heels" and an author's interpretation of this category has been proposed. During the analysis of these types of traces, the author's differentiation of them into volatile and relevant ones was proposed.
Research implication. The author's interpretation of the "digital footprints noticed "hot on the heels" has been introduced, which is of great theoretical importance for digital forensics. The detailed consideration of certain types of volatile and relevant traces, from a practical point of view, contribute to a more accurate direction of work of investigators and specialists, preserving the maximum evidence potential of the discovered objects.

Keywords: actual footprints, virtual footprints, volatile footprints, digital footprints noticed "hot on the heels", digital footprints noticed "without delay" investigation, traces in cyberspace, electronic digital footprints

Acknowledgements. The study was funded by the Russian Science Foundation grant no. 24-28-00312.

For citation:
Smushkin, A. B. (2025). Digital Footprints Noticed "Hot on the Heels." In*: Moscow Juridical Journal*, 1, 94–102. https://doi.org/10.18384/2949-513X-2025-1-94-102.

Введение

Идея выделения отдельного типа следов в компьютерных устройствах, наряду с идеальными и материальными следами, возникла в криминалистике уже достаточно давно. Первые публикации появились ещё в начале нулевых годов этого века [1; 2]. Однако до настоящего момента нет чёткой дефиниции данной категории следов и даже по вопросу их наименования отсутствует единое мнение – встречаются и *следы технического характера* [3, с. 53, 64, 67], и *компьютерно-технические* [4], и *бинарные* [5], и *виртуальные* [6; 7; 8], и *цифровые* [9; 10], и *информационные* [11], и *электронные* [12], и *электронно-цифровые* [13]. М. М. Менжега вообще использует термин «следы использования компьютерной техники», под которым понимает чрезвычайно широкую категорию, что делает невозможным их отнесение к одной из определённых групп следов (материальных, идеальных или виртуальных). Следы такого рода, по его мнению, могут принимать самые разнообразные формы: от распечатанного на бумаге текста до информации в инфракрасных лучах, а также мысленные образы, оставшиеся в памяти очевидца после наблюдения изображения на экране компьютера [14, с. 17].

Не вдаваясь в дискуссию, отметим, что категорией, объединяющей электронные, квантовые и иные виды следов в современных и перспективных информационно-технологических устройствах, являются «виртуальные следы». Основываясь на определении В. А. Мещерякова, можно охарактеризовать виртуальные среды как «взаимосвязанный комплекс материально зафиксированной информации как результат специально организованного выборочного отражения фрагментов окружающей действительности в искусственной среде и знаний о формализованной модели, положенной в основу создания этой инцидентной среды отражения» [8, с. 108].

С учётом малого распространения (на момент подготовки публикации) квантовых, генетических, оптических и иных перспективных компьютерных устройств, необходимо отдельно остановиться, прежде всего, на электронном цифровом виде следов.

Непосредственно электронные цифровые следы – это «следы отражения совер-

шения любых действий (включения, создания, открывания, активации, внесения изменений, удаления) в информационном пространстве именно электронных информационно-технологических устройств, их систем и сетей» [15, с. 93].

Концепция горячих электронных цифровых следов

Отдельно остановимся на таком типе следов, который подлежит безотлагательному исследованию в связи с возможностью организации установления местонахождения злоумышленника, как «горячие следы».

В материальном пространстве при поиске следов в ходе осмотра места происшествия необходимо обращать внимание на эти «горячие следы». Под ними обычно понимаются «хорошо сохранившиеся следы совершения преступления, которое было совершено сравнительно недавно» [16, с. 734]. Условно к горячим следам можно отнести также следы с крайне малым идентификационным периодом.

В киберпространстве можно выделить аналогичную категорию «горячих» электронных цифровых следов, т. е. следов, подлежащих исследованию в неотложном режиме и позволяющих установить местонахождение злоумышленника в киберпространстве с привязкой к материальному пространству, а в некоторых случаях и обнаружить, и задержать его.

«Горячие» электронные цифровые следы могут включать в себя информацию из различных источников: социальных сетей, систем геопозиционирования и т. д. Значение этих следов обусловлено возможностью и перспективностью использования их именно в «в моменте».

Выделим 2 основные группы горячих электронных цифровых следов, которые условно назовём «волатильными» и «актуальными».

Волатильные следы имеют свойство быстрой модификации или уничтожения, вследствие чего подлежат скорейшему безотлагательному выявлению и исследованию.

В первую очередь, это *следы в оперативной памяти*. Оперативной памятью сейчас обладают не только компьютерные, но иные информационно-технологические и периферийные устройства компьютерной системы или сети. В оперативную память подгружаются элементы программ и иные, необходимые для быстрой работы программ, данные, обрабатываемые процессором.

Оперативная память носит энергозависимый характер. При выключении или перезагрузке устройства все следы в этой памяти стираются. Это обуславливает необходимость скорейшего извлечения информации (снятия дампа памяти). Кроме того, следователь должен оценить безопасность энергоснабжения устройства и в случае снижающегося энергозапаса подключить к источнику питания или переносному аккумулятору. В оперативной памяти может быть обнаружена криминалистически релевантная информация о задачах, процессах, открытых файлах, ключах шифрования и т. д.

Далее – это *кэш-память* устройства. Кэш – это высокоскоростное буферное хранилище, один из уровней памяти, содержащее необходимую информацию, к которой происходит частое обращение. Кэш может быть системным (системных служб), пользовательским (кэш приложений), браузерным кэшем, *daily*-кэшем (у мобильных устройств на основе операционной системы *Android*). Следы в памяти кэша могут быть очищены пользователем вручную с помощью запуска программ, а также автоматически запланированным действием программы. В данной буферной памяти могут быть обнаружены криминалистически значимые следы в виде текстовых файлов, медиафайлов и др.

К рассматриваемой категории следов можно отнести также иные, носящие временный характер следы в памяти электронной системы информационно-технологических устройств. Так, значительный объём электронных цифровых следов может быть обнаружен во временных файлах, расположенных в папках *Temp,*

Temporary Internet Files и аналогичных. Их волатильность обусловлена возможностью как «ручной» чистки, так и планового программного запуска обслуживающего оптимизирующего программного комплекса, чистящего временные файлы, закрывающего фоновые приложения и т. д. Поскольку неизвестно установлено ли обслуживание при перезагрузке (включении) компьютера, либо просто с определённой периодичностью (возможно, достаточно короткой), то оптимальным представляется безотлагательное, аналогично снятию дампа оперативной памяти, копирование и исследование данной информации.

Временные файлы создаются некоторыми программами для ускорения работы, что даёт возможность в ходе расследования исследовать автоматически сохранённые тексты, этапы работы конкретных программ, приложений и т. д.

Следует также отдельно выделить категорию *временны́х меток*. Временны́е метки – это метки, фиксирующие совершения тех или иных действий пользователя. Они могут помочь установить хронологию действий пользователя в системе, что будет иметь высокое криминалистическое значение.

Логи (log-файлы) – файлы, в которых ведётся запись журналов работ, конкретных программ, действий пользователей в киберпространстве сети или изолированного устройства и т. д. Логирование подключений может вестись даже на серверах VPN.

Выделяют следующие виды логов:

– *системные* – из них может быть получена информация об основных событиях операционной системы;

– *логи веб-сервера* – могут быть изучены факты регистрации обращений к сайту;

– *логи почтовых служб* – в них фиксируются все активности, связанные с использованием электронной почты, что может иметь высокое криминалистическое значение для фиксации времени направления/получения электронных писем, их адресата и т. д.;

– *логи FTP сервера* – содержат информацию о каждом подключении;

– *логи баз данных* – могут содержать криминалистические значимые сведения о всех транзакциях, запросах и предупреждениях в системах управления базы данных;

– *логи авторизации и аутентификации* – фиксируют процессы входа / выхода, восстановление доступа, и т. д. Криминалистическое значение этой информации заключается в подтверждении или опровержении попыток подбора пароля, попыток взлома системы, входа из неустановленного места, хронологию входа в определённую программу или выхода из неё и т. д.[1]

Важность криминалистического исследования журналов работ из *log*-файлов выделяют многие зарубежные учёные [17; 18; 19; 20].

Можно также выделить и такие волатильные следы, как *исчезающая переписка в мессенджерах*. В настоящее время почти каждый мессенджер содержит расширенный функционал в области сохранения конфиденциальности переписки. Большинство современных мессенджеров имеет опцию временных или исчезающих сообщений. Конечно, имеются экспертные методы восстановления переписки в чатах мессенджеров, использующих даже протоколы *Signal*. Однако в целях более оперативного реагирования, снижения тактического риска, оптимального использования данных горячих следов рекомендуется уделять им повышенное внимание – фиксировать с помощью протоколов осмотра фотографирования, снимков экрана (скриншотов).

Активные на момент начала осмотра *сетевые соединения* могут либо быть разорваны другой стороной или модератором, либо отключиться при обычном выключении компьютера. Следовательно, они также носят волатильный характер и подлежат исследованию в первоочерёдном режиме. Активные сетевые соединения могут быть изучены и зафиксированы с помощью программных комплексов. К отечественным разработкам в сфере сетевой криминалистики, позволяющим фиксиро-

[1] Может иметь значение для подтверждения / опровержения цифрового алиби.

вать и анализировать сетевой трафик, относятся: *PT Network Attack Discovery (NAD)* от *Positive Technologies, ViPNet Coordinator KB* от «Инфотекс», *EtherSensor* от *Microolap*, NTA от «Центра кибербезопасности», Solar NTA от компании «Солар», Гарда от *NDR*, *Kaspersky Anti Targeted Attack (KATA), ATHENA* от *AVSOFT*, «Стетоскоп» и др.[1].

Достаточно большое значение будут иметь также сессионные данные и файлы *cookies*. Эти файлы могут содержать идентификационную информацию, аутентификационные данные, историю действий пользователя, информацию о персональных настройках, статистику пользователя и т. п. Сами файлы создаются системой для ускоренного доступа к сайту с помощью «привязки» к их информации, а не постоянного сбора её заново.

В. В. Худяков и А. А. Ананьев указывают на существование следующих видов *cookie*-файлов:

1) *временные* – такие файлы являются безопасными, т. к. удаляются при выходе пользователя с конкретного сайта;

2) *постоянные* – такие *cookie* остаются на компьютере до того момента, пока их не удалят вручную;

3) *сторонние* или *супер-cookie* – такие *cookie* записываются сторонними доменами более высокого уровня;

4) *evercookie* или *зомби-cookie* – являются самыми опасными из остальных видов *cookie*-файлов, т. к. удалить их практически невозможно [21, с. 244].

Следует отметить, что последние варианты *cookies* могут быть почищены пользователем, однако они имеют функционал восстановления за счёт информации, хранящейся в сети Интернет [22, с. 185–186].

Зарубежные учёные указывают, что принятие или отказ от принятия постоянных файлов *cookie* может также быть связано с психологией пользователя и его личными предпочтениями [23].

Сессионные данные вообще хранятся на сервере только в течение работы пользователя на определённом ресурсе и после завершения сеанса удаляются. Они используются для отслеживания активности пользователя в рамках сессии и обеспечивают более персонифицированный опыт.

Следующая группа горячих электронных цифровых следов имеет повышенное значение именно «в моменте». Условно назовём их «актуальными». К данной группе относятся следы, которые требуют незамедлительной реакции следствия, поскольку отсрочка может привести к потере актуальности этих следов и тактическому риску недостижения планируемого результата, основанного на них следственного действия.

Например, данные геопозиционирования лица имеют несомненное актуальное значение. Геопозиционирование можно проводить как с помощью триангуляции (запросы с трёх вышек сотовой связи с отслеживанием времени отклика и вычислением географических координат), так и с помощью следственных действий, предусмотренных ст. 186.1 УПК РФ «Получение информации о соединениях абонентов абонентских устройств» (информация об обслуживающей станции или месте компьютерного устройства в сети). Однако при наличии в компьютерном устройстве активного модуля *GPS* ГЛОНАСС актуальную информацию о местонахождении можно получить быстрее и точнее.

Так, по уголовному делу о трансграничной перевозке наркотиков было установлено, что наркотические средства из Испании в Россию перемещались на автомобиле, оснащённом *gps*-треккером для слежения, что было эффективно использовано в ходе расследования и доказывания в суде[2].

[1] *См.:* NTA: обзор лучших российских решений для анализа сетевого трафика // Лаборатория Касперского: [сайт]. URL: https://www.securitylab.ru/blog/personal/paragraph/354348.php?utm_referrer=https%3A%2F%2Fya.ru%2F (дата обращения: 15.12.2024).

[2] Приговор Псковского областного суда от 28.02.2017 по делу № 2–1/2017 (2-4/2016;) [Электронный ресурс]. URL: https://actofact.ru/case-60OS0000-2-1-2017-2-4-2016-2016-04-18-2-0/ (дата обращения: 15.12.2024).

Некоторые авторы вообще предлагают ввести новое следственное действие «Получение информации о географических координатах». Так, Х. Х. Рамалданов предлагает следующую редакцию указанной нормы: «Получение информации о географических координатах места нахождения (геолокации) абонента, транспортного средства и (или) абонентского устройства» – следующего содержания:

«1. При наличии достаточных оснований полагать, что информация о географических координатах места нахождения абонента, транспортного средства и (или) абонентского устройства имеет значение для уголовного дела, получение следователем указанной информации допускается на основании судебного решения, принимаемого в порядке, установленном статьёй 165 настоящего Кодекса.

2. Получение информации о географических координатах места нахождения (геолокации) абонента, транспортного средства и (или) абонентского устройства производится в порядке, установленном статьёй 186.1 настоящего Кодекса, с изъятиями, предусмотренными настоящей статьёй.

3. Следователь осматривает представленные сведения, содержащие информацию о географических координатах места нахождения (геолокации) абонента, транспортного средства и (или) абонентского устройства, в порядке предусмотренном ч. 5 ст. 186.1 настоящего Кодекса с указанием географических координат места нахождения (геолокации) абонента, транспортного средства и (или) абонентского устройства и другие данные» [24, с. 276].

Подобные следы могут оставаться как в сотовых мобильных телефонах, так и в иных электронных устройствах (смартчасах, трекерах, системах спутникового мониторинга и контроля АвтоГраф, современных сигнализациях с установкой в автомобиле соответствующего модуля, навигаторах, E-Call системах современных автомобилей и т. д.). Оперативное, в первую очередь, дистанционное исследование этих следов позволит застать объект на месте, а излишняя отсрочка, наоборот, позволит объекту скрыться. При этом выявление основных реперных точек и направления движения позволит прогнозировать траекторию движения заподозренных лиц и итоговую точку маршрута.

Следующая группа следов – это *перехваченный трафик*, *«живые сетевые пакеты»*. Они требуют безотлагательной дешифровки и использования в расследовании. В некоторых случаях с помощью перехваченного трафика можно предотвратить само совершение преступления, с подменой отдельных элементов программного кода определить по отклику IP-адрес преступника и т. д., что, например, может способствовать деанонимизации пользователя Даркнета.

Данные из чатов мессенджеров, онлайн-игр, иных компьютерных приложений могут не только использоваться для доказывания при ретроспективном познании события преступления, но и требовать незамедлительного реагирования в онлайн-режиме. Через подобные чаты могут не только обсуждаться планы преступления, но и координироваться действия группы преступников, отдаваться команды и указания. Сведения о перехваченных данных в ходе снятия информации с технических каналов связи, получения компьютерной информации, контроля записи переговоров, наложения ареста на электронное сообщение и т. д. могут послужить предпосылкой предупреждения или пресечения преступления. Так, по делу № 1-26/2024, рассмотренному Судебной коллегией по делам военнослужащих Верховного Суда Российской Федерации 9 апреля 2025 г., именно переписка в мессенджере «Т…» использовалась для организации пропаганды террористической деятельности[1].

[1] Кассационное определение от 09.04.2025 г. по делу № 1-26/2024 Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации // СудАкт: [сайт]. URL: https://sudact.ru/vsrf/doc/oUP7xbhniM1x/?vsrf-txt=мессенджеры&vsrf-case_doc=&vsrf-lawchunkinfo=&vsrf-date_from=&vsrf-date_to=&vsrf-judge=&_=1751258942506 (дата обращения: 15.12.2024).

В условиях активного взаимодействия можно выявить и исследовать также запросы в поисковые системы маркетплейсов, онлайн-покупки, интерактивные действия.

Технологии анализа горячих электронных цифровых следов должны включать современные методы обработки больших данных и выявления скрытых закономерностей. Скорость анализа также будет иметь большое практическое значение при оперативном реагировании на события преступления. С учётом характеристики электронных цифровых следов при исследовании информационно-технологического устройства нужно обязательно использовать устройство, блокирующее запись (*write breakers*). Сама информация также должна исследоваться не на оригинальном устройстве, а после снятия образа (клона) диска.

Заключение

Таким образом, концепция горячих электронных цифровых следов непосредственно подчёркивает важность крайне аккуратного, но при этом оперативного исследования электронных объектов. Понимание их природы, качество работы, квалификация специалистов являются ключевыми факторами их эффективного использования. Горячие электронные цифровые следы могут оптимизировать работу следователя или специалиста, определить очерёдность исследования следов, обнаружить и идентифицировать подозреваемого и установив временные рамки событий.

ЛИТЕРАТУРА

1. Яковлев А. Н. Теоретические и методические основы экспертного исследования документов на машинных носителях информации: дис. … канд. юрид. наук. Саратов, 2000. 436 с.
2. Мещеряков В. А. Механизм следообразования при совершении преступлений в сфере компьютерной информации // Известия Тульского государственного университета. Современные проблемы законодательства России, юридических наук и правоохранительной деятельности. 2000. № 3. С. 167.
3. Федотов Н. Н. Форензика – компьютерная криминалистика. М.: Юридический Мир, 2007. 481 с.
4. Лыткин Н. Н., Гаврилин Ю. В. Использования компьютерно-технических следов при установлении события преступления // Известия Тульского государственного университета. Серия: Актуальные проблемы юридических наук. 2006. № 15. С. 44–50.
5. Милашев В. А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ // Актуальные вопросы теории и практики раскрытия, расследования и предупреждения преступлений: тезисы конференции. Тула, 2004. С. 34–39.
6. Черкасов В. Н., Нехорошев А. Б. «Виртуальные следы» в «кибернетическом пространстве» // Судебная экспертиза: сборник научных статей. Вып. 2. Саратов: Саратовский юридический институт МВД России, 2003. С. 127–130.
7. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе. М.: Юрлитинформ, 2012. 148 с.
8. Мещеряков В. А. Теоретические основы механизма следообразования в цифровой криминалистике. М.: Проспект, 2022. 176 с.
9. Толстолуцкий В. Ю. Закономерности криминалистической теории отражения, присущие субъективному этапу // Вестник Нижегородского университета им. Н. И. Лобачевского. Серия: Право. 2008. № 2. С. 203–209.
10. Теория информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский, Т. А. Сааков. М.: Проспект, 2022. 254 с.
11. Камалова Г. Г. Криминалистическая методика расследования преступлений в сфере компьютерных технологий // Криминалистика: курс лекций по криминалистике для бакалавров / под ред. М. К. Каминского, А. М. Каминского. Ижевск, 2012. С. 257–279.
12. Ищенко Е. П. Криминалистика: главные направления развития // Сибирские уголовно-процессуальные и криминалистические чтения. 2012. № 1. С. 201–209.
13. Иванов В. Ю. К вопросу о классификации электронно-цифровых следов // Национальная без-

опасность / Nota Bene. 2020. № 3. С. 64–71.
14. Менжега М. М. Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ: автореф. дис. … канд. юр. наук. Саратов, 2005. 22 с.
15. Смушкин А. Б. Цифровизация криминалистической деятельности. М.: КноРусс. 2024. 208 с.
16. Мордюк А. В., Ковригина В. А. Понятие и общие положения методики расследования преступлений «по горячим следам» // Аллея науки. 2020. Т. 1. № 5. С. 734–740.
17. Surina He, Ying Cui, A systematic review of the use of log-based process data in computer-based assessments // Computers & Education. 2025. Vol. 228. P. 105245.
18. A multi-source log semantic analysis-based attack investigation approach / Yubo Song, Kanghui Wang, Xin Sun, Zhongyuan Qin, Hua Dai, Weiwei Chen, Bang Lv, Jiaqi Chen // Computers & Security. 2025. Vol. 150. P. 104303.
19. Fehrer T., Moder L., Röglinger M. An interactive approach for group-based event log exploration // Information Systems. 2025. Vol. 134. P. 102575.
20. Fageeri S. O., Ahmad R. An Efficient Log File Analysis Algorithm Using Binary-based Data Structure // Procedia – Social and Behavioral Sciences. 2014. Vol. 129. P. 518–526.
21. Худяков В. В., Ананьев А. А. Цифровые следы // Криминологический журнал. 2023. № 4. С. 243–246.
22. Чернышев Е. Форма жизни № 4: Как остаться человеком в эпоху рассвета искусственного интеллекта. М.: Альпина Паблишер, 2022. 484 с.
23. Papenmeier F., Halama J., Reichert C. Accepting cookies: Nudging, deceptive patterns and personal preference // Computers in Human Behavior. 2025. Vol. 168. P. 108641.
24. Рамалданов Х. Х. Влияние информационных технологий на процесс доказывания в уголовном судопроизводстве // Пробелы в российском законодательстве. 2023. Т. 16. № 7. С. 273–279.

REFERENCES

1. Yakovlev, A. N. (2000). *Theoretical and Methodological Foundations of the Expert Study of Documents on Machine-Readable Media:* [dissertation]. Saratov (in Russ.).
2. Meshcheryakov, V. A. (2000). Mechanism of Trace Formation in the Commission of Crimes in the Field of Computer Information. In: *Bulletin of Tula State University. Modern Problems of Russian Legislation, Legal Sciences and Law Enforcement*, 3, 167 (in Russ.).
3. Fedotov, N. N. (2007). *Forenzika – Computer Forensics*. Moscow, Legal world publ. (in Russ.).
4. Lytkin, N. N. & Gavrilin, Yu. V. (2006). The Use of Computer Technical Traces in Establishing the Crime Event. In: *Bulletin of Tula State University. Series: Actual Problems of Legal Sciences,* 15, 44–50 (in Russ.).
5. Milashev, V. A. (2004). Problems of Tactics for Searching, Fixing and Removing Traces in Case of Illegal Access to Computer Information in Computer Networks. In: *Current Issues of the Theory and Practice of Disclosure, Investigation and Prevention of Crimes*. Tula, pp. 34–39 (in Russ.).
6. Cherkasov, V. N. & Nekhoroshev, A. B. (2003). "Digital Footprints" in the "Cybernetic Space." In: *Forensic Examination. Iss. 2.* Saratov: Saratov Law Institute of the Ministry of Internal Affairs of Russia, 127–130 (in Russ.).
7. Agibalov, V. Yu. (2012). *Digital Footprints in Forensics and Criminal Proceedings*. Moscow: Yurlitinform publ. (in Russ.).
8. Meshcheryakov, V. A. (2022). *Theoretical Foundations of the Mechanism of Trace Formation in Digital Forensics*. Moscow: Prospect publ. (in Russ.).
9. Tolstolutsky, V. Yu. (2008). Patterns of the Forensic Theory of Reflection Inherent in the Subjective Stage. In: *Bulletin of Lobachevsky State University of Nizhny Novgorod. Series: Law,* 2, 203–209 (in Russ.).
10. Rossinskaya, E. R., Semikalenova, A. I., Ryadovsky, I. A. & Saakov, T. A. (2022). *Theory of Information and Computer Support of Forensic Activities.* Moscow, Prospect publ. (in Russ.).
11. Kamalova, G. G. (2012). Forensic Methodology for Investigating Crimes in the Field of Computer Technology. In: Kaminsky, M. K. & Kaminsky, A. M., eds. *Forensics: Course of Lectures on Forensics for Bachelors*. Izhevsk, pp. 257–279 (in Russ.).
12. Ishchenko, E. P. (2012). Forensics: The Main Directions of Development. In: *Siberian Criminal Procedure and Criminalistic Readings*, 1, 201–209 (in Russ.).
13. Ivanov, V. Yu. (2020). On the Classification of Electronic Digital Footprints. In: *National Security / Nota Bene*, 3, 64–71 (in Russ.).

14. Menzhega, M. M. (2005). *Forensic Problems of Investigating the Creation, Use and Distribution of Malware for Computers:* [dissertation]. Saratov (in Russ.).
15. Smushkin, A. B. (2024). *Digitalization of Forensic Activities*. Moscow, KnoRuss publ. (in Russ.).
16. Mordyuk, A. V. & Kovrigina, V. A. (2020). The Concept and General Provisions of the Methodology for Investigating Crimes "Hot on the Heels." In: *Alley of Science*, 1-5, 734–740 (in Russ.).
17. Surina He & Ying Cui. (2025). A Systematic Review of the Use of Log-Based Process Data in Computer-Based Assessments. In: *Computers & Education*, 228, 105245.
18. Yubo Song, Kanghui Wang, Xin Sun, Zhongyuan Qin, Hua Dai, Weiwei Chen, Bang Lv, Jiaqi Chen. (2025). A Multi-Source Log Semantic Analysis-Based Attack Investigation Approach. In: *Computers & Security,* 150, 104303.
19. Fehrer, T., Moder, L. & Röglinger, M. (2025). An Interactive Approach for Group-Based Event Log Exploration. In: *Information Systems*, 134, 102575.
20. Fageeri, S. O. & Ahmad, R. (2014). An Efficient Log File Analysis Algorithm Using Binary-based Data Structure. In: *Procedia – Social and Behavioral Sciences*, 129, 518–526.
21. Khudyakov, V. V. & Ananyev, A. A. (2023). Digital Traces. In: *Criminological Journal,* 4, 243–246 (in Russ.).
22. Chernyshev, E. (2022*). Life form No. 4: How to Remain Human in the Era of the Dawn of Artificial Intelligence*. Moscow, Alpina Publisher publ. (in Russ.).
23. Papenmeier, F., Halama, J. & Reichert, C. (2025). Accepting Cookies: Nudging, Deceptive Patterns and Personal Preference. In: *Computers in Human Behavior*, 168, 108641.
24. Ramaldanov, Kh. Kh. (2023). Influence of Information Technologies on the Process of Evidence in Criminal Proceedings. In: *Gaps in Russian Legislation*, 16-7, 273–279 (in Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Смушкин Александр Борисович (г. Саратов) – кандидат юридических наук, ведущий научный сотрудник проектного офиса научных программ и исследований, доцент кафедры криминалистики Саратовской государственной юридической академии;
e-mail: skif32@yandex.ru; ORCID: 0000-0003-1619-8325

INFORMATION ABOUT THE AUTHOR

Alexander B. Smushkin (Saratov) – Cand. Sci. (Law), Senior Researcher, Project Office of Scientific Programs and Research, Assoc. Prof., Department of Criminology, Saratov State Law Academy;
e-mail: skif32@yandex.ru; ORCID: 0000-0003-1619-8325