

УДК 343.98

## ЦИФРОВОЙ СЛЕД И ЕГО ЗНАЧЕНИЕ В ПРАКТИКЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Д. А. Свиридов

Могилевский институт МВД Республики Беларусь,  
начальник кафедры уголовного процесса и криминалистики

**Аннотация.** В статье рассматриваются подходы к понятию цифрового следа. В настоящее время расследование практически каждого уголовного дела связано с деятельностью по обнаружению, фиксации, изъятию и использованию цифровых следов, содержащих информацию об обстоятельствах совершения общественно опасного деяния. В статье устанавливаются особенности цифровых следов, их виды, носители и значение для практики расследования уголовных дел.

**Ключевые слова:** цифровой след, преступление, расследование, криминалистика, носитель цифровой информации.

**Annotation.** The article discusses approaches to the concept of a digital footprint. Currently, the investigation of almost every criminal is associated with the activity of detecting, fixing, seizing and using digital traces containing information about the circumstances of the commission of a socially dangerous act. The article establishes the features of digital traces, their types, carriers and significance for the practice of investigating criminal cases.

**Keywords:** digital trace, crime, investigation, criminology, digital information carrier.

В современном мире цифровые технологии играют все большую роль в нашей жизни. Они помогают нам общаться, работать, учиться и развлекаться. Однако они также оставляют цифровые следы, которые могут быть использованы при расследовании преступлений. В целом научно-технический прогресс приводит не только лишь к развитию науки и техники в целях развития общества, но также к использованию современных достижений при совершении общественно опасных деяний. Исследователи отмечают, что в настоящее время практически каждое 20-е преступление — это преступление, совершенное с использованием глобальной сети Интернет [1, с. 27].

Белорусское общество, для которого характерны все основные тенденции, как и для остальных развитых стран, все быстрее трансформируется в общество цифровое, а в общественной жизни нарастает наличие цифровых технологий. В этой связи следует отметить достаточно большое количество вошедших в обращение новых дефиниций, среди которых необходимо отметить понятие «цифровой след», т. е. информации, которая сохраняется после совершения действий в мобильных сетях, глобальной сети Интернет, локальных сетях, а также отдельных технических устройствах (так называемый цифровой

отпечаток). Не оспаривая различные подходы к даваемым определениям данного понятия, видится необходимым отметить ту основу, которая характерна для большинства из них, основанное на традиционном криминалистическом понимании следа, т. е. это любые изменения среды под влиянием преступления [2; 3]. Цифровые следы — это информация, которая остается после использования электронных устройств и сервисов. Это могут быть данные о звонках, сообщениях, посещенных сайтах, использованных приложениях, фотографиях и видео, а также о местоположении устройства в определенный момент времени. Все эти данные могут помочь правоохранительным органам в расследовании преступлений.

Вместе с тем невозможно не остановиться на тех особенностях, которые характерны исключительно для цифрового следа. Так, прежде всего это наличие особой информационной среды, которой присуще сохранение такого рода следов. Далее следует отметить уникальную физическую структуру цифрового следа, которая представляет собой сохранившиеся сигналы, которые возможно декодировать и представить в виде понятных файлов. И наконец, особенность существования цифрового следа на цифровых и иных физических носителях информации. То есть, по сути, цифровой след — это системное структурированное изменение цифровой среды, хранящееся на цифровых или физических носителях.

Видится возможным детализировать перечень таких носителей:

- устройства мобильной связи;
- компьютеры и ноутбуки;
- планшеты;
- платежные карты;
- электронные устройства (например, медицинские приборы или автомобильные датчики);
- камеры видеонаблюдения;
- информационные базы данных;
- магнитные проездные документы;
- социальные сети и мессенджеры;
- электронная почта;
- чипизованные электронные товарные бирки [4, с. 78];
- банковские карты и платежные системы;
- GPS-навигаторы и другие системы определения местоположения;
- облачные сервисы и хранилища данных и др.

Одним из примеров использования цифровых следов является анализ мобильных телефонов. В современном мире люди почти всегда носят свои телефоны с собой, и они стали неотъемлемой частью нашей жизни. Мобильные

телефоны могут быть использованы для определения местоположения пользователя в определенный момент времени, а также для анализа его коммуникаций, например через текстовые сообщения или социальные сети. Еще одним примером использования цифровых следов является анализ видеозаписей. Видеокамеры установлены в различных местах, например на улицах городов, в магазинах или на станциях метро. Видеозаписи могут быть использованы для выявления преступлений, например грабежей и иных противоправных посягательств.

Цифровые следы также могут быть использованы для анализа данных, собранных с помощью электронных устройств. Например, медицинские устройства могут быть использованы для сбора информации о здоровье человека, а автомобильные датчики могут быть использованы для анализа стиля вождения.

Одним из главных преимуществ использования цифровых следов при расследовании уголовных дел является возможность получения точной и объективной информации. Это помогает правоохранительным органам принимать более обоснованные решения и улучшать качество расследования.

Однако, как и любая другая технология, цифровые следы имеют свои недостатки. Они могут быть использованы для вмешательства в личную жизнь граждан, могут быть подвержены взлому или другим видам кибератак, что может привести к утечке конфиденциальной информации и нарушению прав человека на конфиденциальность.

Цифровые следы имеют первостепенное значение не только при расследовании виртуальных киберпреступлений, но и при работе по сбору доказательств по другим видам правонарушений. Значение анализа цифровых следов в криминалистических целях трудно переоценить: с помощью специальных автоматизированных систем возможно осуществлять сбор информации об интернет-активности лица, совершившего преступление (фиксируются места посещения интернет-ресурсов, области интересов, объекты платежей, интернет-переписка и прочая информация). На основании массива собранных цифровых следов современные алгоритмизированные системы имеют возможность, отсеивая информационный шум, создать так называемый пузырь фильтров — эксклюзивную версию виртуального пространства человека. Существенную часть «цифровых следов» образуют персональные данные. Полученная информация может выступать ценным источником дополнительных сведений о человеке или группе лиц, поэтому охраняется от случайного распространения законодательством Республики Беларусь.

Одним из самых распространенных видов цифровых следов являются метаданные, которые представляют собой информацию об информации.

Например, метаданные фотографии могут содержать информацию о дате и времени ее создания, модели камеры, настройках экспозиции и т. д. Эта информация может быть использована для определения местоположения и времени события.

Другим видом цифровых следов являются данные о местоположении. Современные смартфоны и другие устройства постоянно отслеживают местоположение пользователя. Эта информация может быть использована для определения места нахождения подозреваемого в момент совершения преступления или доказывания непричастности лица к его совершению.

Также цифровые следы могут быть использованы для анализа коммуникаций. Например, могут быть изучены записи звонков и сообщений, чтобы определить, кто общался с подозреваемым и о чем они говорили. Цифровые следы также могут быть использованы для анализа социальных сетей. Социальные сети содержат огромное количество информации о пользователях, которая может быть использована для раскрытия преступлений. Например, фотографии и видео из социальных сетей могут быть использованы для определения местоположения и времени события.

В заключение следует отметить, что цифровые следы являются важным инструментом при расследовании преступлений. Они помогают правоохранительным органам в выявлении подозреваемых и раскрытии преступлений. Вместе с тем использование цифровых следов должно осуществляться в соответствии с законодательством и уважением к правам человека. В целом использование цифровых следов при расследовании уголовных дел имеет свои плюсы и минусы. Однако в современном мире, где технологии играют все большую роль, правоохранительным органам необходимо уметь использовать цифровые следы для более эффективного расследования преступлений.

---

1. Гимазетдинова А. Р. Особенности обнаружения, изъятия и фиксации цифровых следов // Студенч. южноурал. криминалистич. чт. : сб. материалов Всерос. науч.-практ. конф., Уфа, 2–3 дек. 2021 г. Уфа : Науч.- исследоват. ин-т проблем правового государства, 2022. С. 26–30. [Вернуться к статье](#)

2. Гужаева В. А., Прокофьева Е. В., Прокофьева О. Ю. Преступность в сети Интернет: криминологические характеристики // Вестн. эконом. безопасности. 2019. № 4. С. 111–114. [Вернуться к статье](#)

3. Скобелин С. Ю. Цифровая криминалистика: объект и направления развития // Российский следователь. 2020. № 4. С. 42–44. [Вернуться к статье](#)

4. Железняк А. С. Криминалистика: тактико-методические основы уголовного судопроизводства : учеб. пособие. 2-е изд., стер. М. : МГИУ, 2008. 126 с. [Вернуться к статье](#)