



СОВРЕМЕННЫЕ МЕТОДЫ ФИКСАЦИИ И АНАЛИЗА ЦИФРОВЫХ СЛЕДОВ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Погорелова Ангелина Николаевна

Горбунова К.С.

научный руководитель: Саюшкина Е.В.

канд. юр. наук, доцент

Оренбургский институт (филиал) ФГАОУ ВО «Московского государственного
юридического университета имени О. Е. Кутафина (МГЮА)»

Россия, г. Оренбург

Аннотация. В статье рассматривается современное состояние криминалистического исследования цифровых следов, образующихся при совершении киберпреступлений. Анализируются особенности цифровых следов как нового вида вещественных доказательств, требующего специальных методов изъятия и закрепления. Особое внимание уделяется технологиям создания посекторных копий носителей, восстановлению удаленной информации и соблюдению процессуальных норм при работе с электронными уликами.

Ключевые слова: Криминалистика, цифровые следы, киберпреступление, компьютерная экспертиза, фиксация доказательств, восстановление данных, метаданные, информационная безопасность, расследование.

MODERN METHODS OF RECORDING AND ANALYZING DIGITAL TRACES IN THE INVESTIGATION OF CYBERCRIMES

Pogorelova Angelina Nikolaevna

Gorbunova K.S.

scientific Advisor: **Sayushkina E.V.**

Candidate of Legal Sciences, Associate Professor

Orenburg Institute (Branch) of the Federal State Autonomous Educational Institution of Higher
Education "Moscow State Law University named after O. E. Kutafin (MSLA)"

Russia, Orenburg

Abstract. The article examines the current state of forensic research of digital traces formed during cybercrimes. It analyzes the features of digital traces as a new type of physical evidence that requires special methods of seizure and consolidation. Special attention is paid to the technologies of creating sector-by-sector copies of media, restoring deleted information, and compliance with procedural norms when working with electronic evidence.

Keywords: Forensics, digital traces, cybercrime, computer expertise, evidence fixation, data recovery, metadata, information security,

В настоящее время сложно представить наш современный мир без компьютерной техники, сотового телефона и сети Интернет. Они представляют собой обязательное условие улучшения качества жизни, но наряду со своей позитивностью, они стремительно подвергают опасности жизнь и конфиденциальность данных человека и общества в целом. Стремительное развитие информационных технологий и широкое распространение цифровых платформ радикально изменили криминогенную ситуацию в мире-зафиксирован резкий скачок преступлений с использованием IT-технологий.

Само понятие «киберпреступность» появилось за рубежом. В 2000 году на десятом Конгрессе ООН по предупреждению преступности и обращению с правонарушителями киберпреступления разделили на пять категорий: несанкционированный доступ к устройству; повреждение компьютерных данных или программ; саботаж для нарушения работы компьютерной системы или сети; несанкционированный перехват данных внутри системы или сети; компьютерный шпионаж.

В России киберпреступности посвящена глава 28 УК РФ об ответственности за преступления в сфере компьютерной информации.

Всемирный процесс цифровизации и усиленный рост подобных преступлений привел к появлению в Следственном комитете Российской Федерации отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий. Данный отдел начал свою работу с декабря 2019 года. Ведь результативность следствия по указанным категориям дел напрямую зависит от качества фиксации и изучения массива цифровых данных, остающихся после совершения правонарушения.

В криминалистической литературе можно увидеть различные подходы ученых к пониманию и содержанию "виртуального следа". А.Б. Смушкин данный вид следа определяет как результат "совершения любых действий в информационном пространстве компьютерных и иных цифровых устройств, их сетей и систем". В.А. Мещеряков под виртуальными следами понимает "любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации".

Среди основных свойств электронно-цифровых следов можно выделить: возможность осуществления процедуры неограниченного копирования без нарушения целостности; первоисточника информации, а так же несложную процедуру быстрого изменения или уничтожения, как первичной информации, так и её копий.



Расследование преступлений, совершенных с использованием информационно-телекоммуникационных технологий, невозможно без глубокого понимания природы цифровых следов. Как было отмечено ранее, ключевым свойством таких следов является их нематериальность и уязвимость. В отличие от традиционных трасологических или дактилоскопических отпечатков, цифровой след не может быть просто «изъят» в классическом понимании этого процесса. Следователь и специалист имеют дело не с физическим объектом, а с информацией, закодированной в виде последовательности электрических импульсов или состояний ячеек памяти. В связи с этим фундаментальное значение приобретает процедура копирования информации. Законодательство Российской Федерации, в частности Уголовно-процессуальный кодекс, предусматривает возможность изъятия носителей информации, однако на практике это не всегда целесообразно. Изъятие сервера коммерческой организации или критически важного узла автоматизированной системы управления может парализовать работу предприятия, нанеся ущерб, несоизмеримый с самим преступлением. Именно поэтому современная криминалистика делает акцент на производстве копирования цифровой информации непосредственно на месте происшествия. Процесс фиксации цифровых следов начинается с осмотра места происшествия, которым может выступать не только помещение с компьютерной техникой, но и виртуальное пространство. Ключевым требованием на данном этапе является обеспечение неизменности данных. Любое включение или выключение компьютера, подключение к сети или даже простое нажатие клавиши может привести к изменению временных меток файлов, удалению временных данных или запуску механизмов шифрования, предусмотренных злоумышленником.¹ Поэтому современным стандартом является работа с «живыми» системами, когда эксперты проводят анализ оперативной памяти до выключения питания. В оперативной памяти хранятся ключевые сведения: пароли в открытом виде, запущенные вредоносные программы, данные о сетевых соединениях. Для извлечения этой информации используются специализированные программно-аппаратные комплексы, позволяющие создать точный образ памяти без внесения изменений в систему.

Технические методы фиксации: от копирования битов до создания образов носителей

После завершения работы с энергозависимыми данными перед криминалистом встает задача изъятия информации с постоянных носителей — жестких дисков, твердотельных накопителей, карт памяти. Традиционное копирование файлов через операционную систему здесь неприменимо, так как оно не позволяет восстановить удаленную информацию и не фиксирует служебные области диска. Современная криминалистика использует метод побитового (посекторного) копирования. Данный метод подразумевает создание точного образа

¹ Россинская Е.Р. Криминалистика: учебник для вузов. — М.: Норма, 2020. — С. 412.



диска — файла, содержащего в себе полную копию всей последовательности битов исходного носителя. Для обеспечения достоверности и проверки неизменности полученной копии применяется технология хеширования. Суть её заключается в математическом вычислении уникального контрольного кода (хеш-суммы) исходного носителя и созданной копии.² Если хеш-суммы совпадают, это является криминалистически значимым доказательством того, что копия полностью аутентична оригиналу и не подвергалась фальсификации в процессе следствия. Данная процедура строго фиксируется в протоколе следственного действия, что позволяет в дальнейшем использовать полученный образ в качестве доказательства в суде. Для работы с такими образами используются аппаратные блокираторы записи. Это устройства, которые подключаются между исследуемым диском и компьютером эксперта и аппаратно блокируют любые команды на запись, гарантируя, что ни один бит информации не будет изменён в процессе экспертизы.

Создание образа — это только первый этап. Основная сложность заключается в анализе гигантских массивов данных, которые могут исчисляться терабайтами. Современные методы анализа базируются на использовании специализированного криминалистического программного обеспечения. Такие программы позволяют автоматизировать поиск ключевых слов, восстановление удаленных файлов, анализ структуры папок и временных характеристик. Одним из важнейших направлений является анализ метаданных. Метаданные — это данные о данных. Каждый цифровой файл (фотография, документ) содержит скрытую информацию о дате и времени создания, редактирования, об авторе, модели устройства, на котором он был создан, и даже о географических координатах съемки. Анализ метаданных часто позволяет установить точное местонахождение преступника в момент совершения противоправного действия или выстроить хронологию событий. Особое место занимает анализ интернет-трафика и сетевых соединений. В условиях, когда преступления совершаются через глобальную сеть, важным источником доказательств являются логи провайдеров и данные о сетевых пакетах. Анализ этих данных позволяет проследить путь информации от отправителя к получателю, установить адреса используемых устройств и, несмотря на использование средств анонимизации, зачастую вывести на конкретного пользователя.

Проблема обеспечения целостности и допустимости доказательств

Несмотря на развитие технических средств, ключевой проблемой остается юридическая сила полученных доказательств. Процесс работы с цифровыми следами должен быть не только технически грамотным, но и процессуально безупречным. Любая ошибка в оформлении — отсутствие понятий при осмотре, некорректное описание изъятого оборудования в протоколе, неисправность блокиратора записи — может привести к тому, что суд признает доказательство

² Смушкин А.Б. Виртуальные следы в криминалистике // Законность. — 2012. — № 8. — С. 43.



недопустимым.³ В связи с этим современная криминалистика выработала строгие стандарты так называемой «цепочки сохранности». Данный принцип подразумевает документальное подтверждение того, кто, когда, при каких обстоятельствах и с помощью каких средств имел доступ к цифровым доказательствам с момента их изъятия до момента рассмотрения дела в суде. Любой разрыв в этой цепочке ставит под сомнение подлинность улик. Для соблюдения этого принципа активно внедряются технологии распределенного реестра, позволяющие фиксировать неизменность данных на всех этапах следствия. Однако на данный момент основным инструментом остается строгое соблюдение норм уголовно-процессуального законодательства и привлечение квалифицированных специалистов для участия в следственных действиях.

Перспективы развития методов анализа

Развитие технологий не стоит на месте, и криминалистика вынуждена постоянно адаптироваться к новым вызовам. Широкое распространение технологий шифрования и анонимных сетей требует от специалистов применения методов криптоанализа и разработки способов легального получения ключей доступа. Всё чаще объектами исследования становятся не только компьютеры, но и устройства интернета вещей — «умные» колонки, бытовая техника, автомобильные системы, которые также накапливают огромные массивы данных о действиях и привычках человека. Активно внедряются методы искусственного интеллекта для обработки больших данных. Нейросети способны анализировать миллионы страниц текстовой переписки или изображений за короткое время, выявляя скрытые связи и закономерности, которые человек мог бы искать годами. Однако использование таких методов ставит новые этические и правовые вопросы о допустимости машинного анализа в доказывании.

Таким образом, современная криминалистика в сфере киберпреступлений представляет собой сложный симбиоз юриспруденции и высоких технологий. Успех расследования напрямую зависит от способности следствия своевременно осваивать и внедрять в практику новейшие методы фиксации и анализа цифровых следов, неукоснительно соблюдая при этом процессуальные нормы, гарантирующие защиту прав всех участников уголовного судопроизводства.

Список литературы:

1. Россинская Е.Р. Криминалистика: учебник для вузов. — М.: Норма, 2020. — С. 412.
2. Смушкин А.Б. Виртуальные следы в криминалистике // Законность. — 2012. — № 8. — С. 43.

³ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 11.10.2024), ст. 81.1, 164.



3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 11.10.2024), ст. 81.1, 164.
4. Шевченко Е.С. О криминалистической трактовке понятия «киберпреступность» // Информационное право. 2014. № 3 (39).
5. Болтенкова Ю.В. Особенности расследования преступлений, совершаемых с использованием it-технологий в сфере компьютерной информации // Поколение будущего: Взгляд молодых ученых — 2022: сборник научных статей 11-й Международной молодежной научной конференции, Курск, 10–11 ноября 2022 года. Том 2. — Курск: Юго-Западный государственный университет, 2022. С. 170–174.