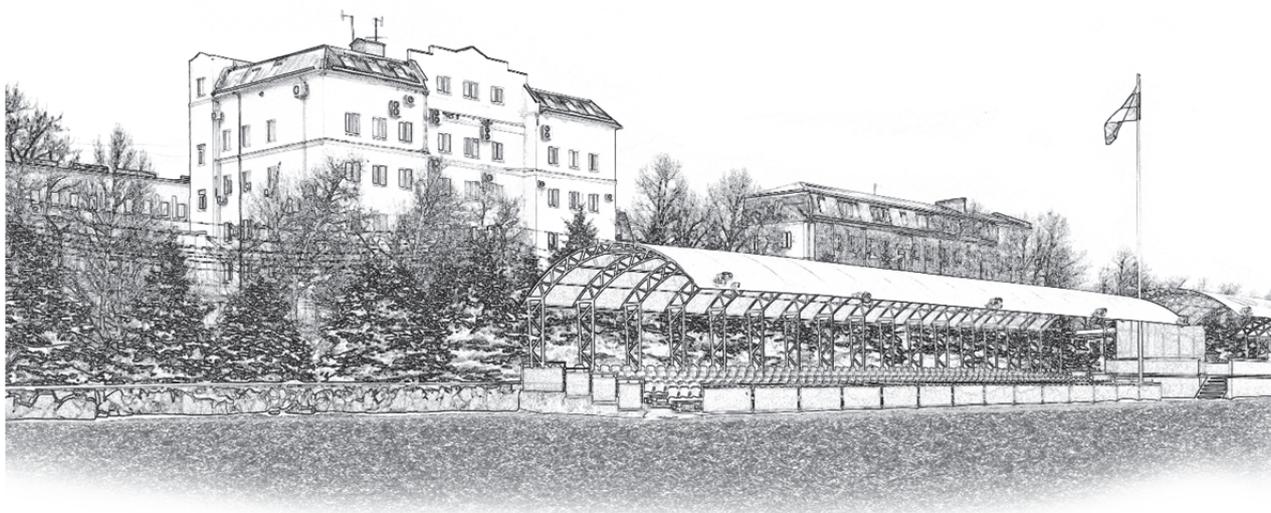




Краснодарский университет МВД России

**ОСОБЕННОСТИ ПОЛУЧЕНИЯ
ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ
С ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ**



Краснодар
2024

Краснодарский университет МВД России

**ОСОБЕННОСТИ ПОЛУЧЕНИЯ
ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ
С ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ**

Методические рекомендации

Краснодар
2024

УДК 343
ББК 67.5
О-754

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Рецензенты:

В. Ю. Хаскина, кандидат юридических наук (Волгоградская академия
МВД России);

П. А. Фаниев (Главное управление МВД России по Краснодарскому
краю).

Авторы:

*Е. В. Афанасьев, В. Р. Арутюнян, Е. С. Бычкова, К. В. Протасов,
А. В. Брылевский.*

Особенности получения доказательственной информации
О-754 с электронных носителей : методические рекомендации / Е. В. Афа-
насьев, В. Р. Арутюнян, Е. С. Бычкова и др. – Краснодар : Краснодар-
ский университет МВД России, 2024. – 18 с.

ISBN 978-5-9266-2074-7

Рассматриваются правовые основы доказательной информации на электронных носителях информации. Приводятся разнообразные методы и процедуры сбора таких доказательств с различных типов цифровых устройств.

Для профессорско-преподавательского состава, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 343
ББК 67.5

ISBN 978-5-9266-2074-7

© Краснодарский университет
МВД России, 2024

Предисловие

Актуальность методических рекомендаций обусловлена резким ростом использования электронных носителей информации в современном обществе. С каждым днем объем цифровых данных увеличивается, и электронные носители становятся неотъемлемой частью практически всех сфер деятельности. Электронные носители представляют собой устройства или среды, используемые для хранения, передачи и обработки данных в цифровом формате. К ним относятся: жесткие диски (HDD), твердотельные накопители (SSD), флеш-накопители (USB), оптические диски (CD, DVD, Blu-ray), карты памяти (SD, microSD), облачные хранилища (Google Drive, Dropbox и др.), а также социальные сети и мессенджеры. Указанные носители могут содержать разнообразные данные, включая текстовые документы, изображения, видео, аудиофайлы, программное обеспечение и т. д.

В методических рекомендациях описаны некоторые современные методы работы с электронными носителями информации. Следует подчеркнуть, что область электронных доказательств постоянно развивается и специалистам в этой сфере необходимо постоянно обновлять свои знания и следить за изменениями в законодательстве. Правильное соблюдение правовых аспектов в работе с электронными доказательствами обеспечивает справедливость и точность в судебных процессах, что важно для общества в целом.

Знание видов и основных характеристик электронных носителей информации дает возможность правильно обнаружить, зафиксировать и изъять электронный носитель, содержащий значимую для расследования уголовного дела информацию, а также при необходимости провести предварительные исследования непосредственно на месте его обнаружения и далее качественно произвести судебную компьютерную экспертизу в условиях экспертной лаборатории с применением современного ПО.

Материалы могут представлять определенный интерес при составлении лекционных курсов по таким дисциплинам, как «Методы получения доказательств с электронных носителей», «Методы получения доказательственной информации с электронных носителей».

Теоретическая значимость методических рекомендаций заключается в обобщении ранее издававшегося теоретического материала, доведения до читателя актуальных терминов и определений по рассматриваемой теме и практических наработок экспертно-криминалистических подразделений системы МВД России. Актуальность методических рекомендаций заключается во внедрении практико-ориентированного подхода в изучение данной дисциплины.

1. Правовые основы доказательственной информации на электронных носителях

В эпоху цифровых технологий электронные носители информации получили широкое распространение, формируя то, как мы общаемся, получаем доступ к информации, ведем бизнес и храним записи. Понимание концепции и различных типов электронных носителей информации важно для всех, кто занимается сбором доказательственной информации, судебными разбирательствами, информационными технологиями и цифровой криминалистикой. Эта теоретическая часть посвящена фундаментальным аспектам электронных данных их определению, значению и разнообразным формам, которые они могут принимать в современном обществе.

Электронные носители информации, часто называемые просто «цифровыми носителями информации», охватывают широкий спектр устройств, форматов и платформ. Эти средства произвели революцию в том, как мы общаемся и взаимодействуем с данными, коренным образом изменив ландшафт управления информацией, юридическую практику и ведение бизнеса. Понимание концепции и типов электронных носителей информации имеет решающее значение, поскольку они служат основой для понимания того, как генерируется, хранится и передается доказательственная информация в цифровом мире.

Электронные носители, по сути, представляют собой цифровые или электронные каналы, используемые для передачи, хранения и обработки информации. Они отличаются от традиционных аналоговых форм средств массовой информации, таких как печать, радио и телевидение, которые используют физические, осязаемые средства для передачи данных. Электронные носители, с другой стороны, имеют дело с информацией в двоичной форме, где данные представлены в виде последовательности из 0 и 1. Такое преобразование в цифровой формат дает множество преимуществ, включая простоту дублирования, манипулирования и передачи, а также эффективное хранение и извлечение информации.

По своей сути электронные носители информации обладают следующими значимыми характеристиками:

1. Способность хранить большие объемы данных. Современные носители могут иметь емкость от нескольких гигабайт до нескольких терабайт и даже петабайт в случае облачных хранилищ.

2. Время, необходимое для чтения или записи данных. Твердотельные накопители (SSD) обычно обеспечивают более высокую скорость доступа по сравнению с традиционными жесткими дисками (HDD).

3. Способностью сохранять данные без потерь в течение длительного времени. Некоторые носители, такие как SSD, менее подвержены механическим повреждениям по сравнению с HDD.

4. Возможностью легко переносить данные между устройствами. Флеш-накопители и карты памяти особенно удобны для этой цели.

5. Безопасностью

6. Совместимостью, т.е. способностью работать с различными устройствами и операционными системами. Например, USB-накопители обычно совместимы с большинством компьютеров и мобильных устройств.

Эти характеристики делают электронные носители информации незаменимыми в современном мире для хранения, передачи и обработки данных.

Типы электронных носителей информации

Электронные носители информации бывают различных форм, каждая из которых предназначена для определенных функций и применений. Понимание этих типов имеет решающее значение для понимания широты цифровых источников, доступных для получения доказательственной информации. В следующих разделах представлен обзор основных типов электронных носителей. Вот краткий обзор основных типов электронных носителей информации:

1. Персональные компьютеры (ПК): Персональные компьютеры являются одной из наиболее распространенных форм электронных носителей информации. Они включают в себя настольные компьютеры, ноутбуки и планшеты и служат центром для различных видов деятельности, от личного общения до задач, связанных с работой.

2. Смартфоны и мобильные устройства: В эпоху мобильных технологий смартфоны и планшеты стали жизненно важными электронными носителями информации. Эти устройства используются для связи, доступа к онлайн-контенту, сбора цифровых доказательств с помощью встроенных камер и многого другого.

3. Серверы и центры обработки данных: Серверы и центры обработки данных служат основой цифрового мира. Они хранят огромные объемы данных и размещают веб-сайты, приложения и облачные сервисы. Сбор доказательств с серверов имеет решающее значение в юридических процессах и расследованиях.

4. Облачные хранилища и сервисы: Облачные решения для хранения данных, такие как Google Диск, iCloud и Dropbox предлагают удобные способы хранения, совместного использования и доступа к данным онлайн. Однако их удобство создает проблемы с точки зрения поиска данных и аутентификации в правовом контексте.

5. Платформы социальных сетей: Платформы социальных сетей, включая Facebook (Meta), Twitter, Instagram и LinkedIn, являются многочисленными источниками цифровых данных. Они содержат огромное ко-

личество информации в виде текста, изображений, видео и многого другого, что делает их неотъемлемой частью многих расследований.

6. Сетевые устройства и Интернет вещей (IoT): Распространение сетевых устройств, от интеллектуальных приборов до камер наблюдения, расширило спектр потенциальных источников доказательственной информации. Эти устройства непрерывно собирают и передают данные, которые могут иметь отношение к расследованиям.

7. Базы данных и корпоративные системы: Крупные организации и учреждения поддерживают базы данных и корпоративные системы для управления своей деятельностью. Эти системы содержат критически важные записи, которые могут быть запрошены в качестве цифровых доказательств в ходе судебных разбирательств.

8. Электронная почта и службы обмена сообщениями: Электронная почта (e-mail) остается основным способом общения в эпоху цифровых технологий. Платформы электронной почты, а также приложения для обмена сообщениями, такие как WhatsApp и Signal, являются богатыми источниками доказательственной информации.

9. Цифровые документы и файлы: Различные типы документов, такие как текстовые файлы, электронные таблицы, презентации и изображения, хранятся в цифровом виде. Эти документы могут иметь значительную доказательственную ценность и необходимы для документирования процессов обнаружения в ходе судебных разбирательств.

10. Системы наблюдения и безопасности: Камеры замкнутого телевидения (CCTV) и другие системы безопасности записывают видеоматериалы, которые могут иметь решающее значение в расследованиях. Эти цифровые видео доказательства в настоящее время широко распространены как в государственном, так и в частном секторах.

11. Финансовые системы и транзакции: Финансовые записи, такие как банковские транзакции, электронные платежи и транзакции с криптовалютой, имеют решающее значение при проведении финансовых расследований и расследовании дел о мошенничестве.

12. Носимые технологии: Носимые устройства, такие как умные часы и фитнес-трекеры, собирают персональные данные, которые могут иметь отношение к случаям получения травм, страховым случаям и многому другому.

13. Игровые и развлекательные системы: Игровые приставки и потоковые платформы являются дополнительными электронными носителями информации. Эти платформы могут содержать журналы чатов, взаимодействия пользователей и другие соответствующие данные.

14. Публичные и частные сети: Локальные вычислительные сети (LAN) и глобальные вычислительные сети (WAN), используемые организациями, учреждениями и частными лицами, играют определенную роль в передаче и хранении цифровых данных.

15. Жесткие диски (HDD) одни из самых распространенных типов носителей, используемых для хранения данных в компьютерах и серверах. Они могут иметь объем памяти от нескольких гигабайт до многих терабайт.

16. Флэш-накопители (USB) компактные устройства для хранения и передачи данных. Они популярны благодаря своей миниатюрности, низкой стоимости и удобству использования.

17. Твердотельные накопители (SSD) быстрые и надежные устройства для хранения данных, которые используют флэш-память. Они имеют высокую скорость чтения и записи данных.

18. Оптические диски (CD, DVD, Blu-ray), используются для хранения больших объемов данных, таких как фильмы, музыка и программное обеспечение. Эти носители долговечны и надежны.

19. Магнитные ленты применяются для архивного хранения данных. Они могут хранить большие объемы информации и используются в основном в корпоративных средах.

20. Криптокошельки – это цифровые кошельки, которые позволяют хранить, отправлять и получать криптовалюты, такие как биткойн, эфириум и другие. Такими криптокошельками могут быть:

- Аппаратные кошельки – физические устройства, которые хранят ваши приватные ключи офлайн, обеспечивая высокий уровень безопасности. Примеры: Ledger, Trezor.

- Программные кошельки – приложения, которые можно установить на компьютер или смартфон. Они могут быть десктопными, мобильными или веб-кошельками. Примеры: Exodus, Electrum, Mycelium.

- Онлайн-кошельки- хранят ваши приватные ключи на серверах компании, предоставляющей услуги кошелька. Они удобны для быстрого доступа, но менее безопасны по сравнению с аппаратными и программными кошельками. Примеры: Coinbase, Blockchain.info.

- Мультиподписные кошельки- требуют нескольких подписей для проведения транзакции, что повышает безопасность. Они могут быть как программными, так и аппаратными.

Современны плацдарм электронных устройств огромен и динамичен, он постоянно развивается, адаптируясь к технологическим достижениям и меняющемуся поведению пользователей. Понимание типов и функций электронных носителей информации имеет основополагающее значение для работы с цифровыми доказательствами. Будь то в области юриспруденции, цифровой криминалистики, информационных технологий или информационной безопасности, владение навыками идентификации, сбора и анализа цифровых доказательств из различных электронных медиа-источников имеет важное значение. Эта теоретическая часть содержит базовые знания, необходимые для того, чтобы ориентироваться в сложностях цифровой эпохи и использовать потенциал электронных носителей

информации в поисках доказательной информации. Это подчеркивает постоянно растущее значение электронных носителей информации в современном обществе и их роль в формировании будущего управления информацией и правовых процессов.

Электронные носители информации как источник доказательств

В эпоху, определяемую цифровой трансформацией, электронные носители информации стали центральным источником доказательств в судебных разбирательствах, расследованиях и определенной формой управления информацией. Значение электронных носителей информации заключается в их способности улавливать, хранить и передавать огромные объемы информации, часто играющей ключевую роль в установлении фактов и обосновании утверждений. Важное значение играет ключевая роль электронных носителей информации как источников доказательств, их важность, допустимость в суде, а также проблемы, которые они создают в правовом поле.

Само появление электронных носителей информации произвело революцию в том, как мы создаем, храним и распространяем информацию. Эта цифровая революция породила множество устройств, платформ и технологий, которые в совокупности формируют основу современной коммуникации и управления данными. В основе этой цифровой трансформации лежит признание того, что электронные носители информации служат не только инструментами взаимодействия, но и настоящими источниками фактических данных.

Следует также уделить внимание значению электронных носителей информации как источников доказательств. Значение электронных носителей информации как источников фактических данных многогранно, что обусловлено присущими им характеристиками и воздействием на общество:

Электронные носители информации играют важную роль как источники доказательств в различных сферах, таких как право, бизнес и наука. Вот несколько ключевых аспектов их значимости:

1. Электронные данные могут быть более точными и достоверными по сравнению с бумажными документами, так как они часто содержат метаданные, такие как время создания и изменения файла.

2. Электронные носители могут хранить огромные объемы информации, включая текстовые документы, изображения, видео и аудиофайлы. Это позволяет собирать и анализировать данные из различных источников.

3. Электронные данные легко копировать, передавать и хранить. Это упрощает процесс обмена информацией и делает ее доступной для анализа и использования в различных контекстах.

4. Современные технологии позволяют защищать электронные данные с помощью шифрования и других методов безопасности, что делает их надежным источником доказательств.

5. Электронные носители информации способствуют развитию цифровой экономики и общества, улучшая доступ к информации и способствуя прозрачности и подотчетности.

Эти характеристики делают электронные носители информации незаменимыми в современном мире, особенно в контексте юридических и деловых процессов.

Использование электронных носителей информации в суде является важным аспектом цифровой криминалистики и юридической практики. На их допустимость в качестве доказательств влияют несколько ключевых факторов:

- Аутентичность. Должно быть доказано, что данные на электронном носителе не были изменены или подделаны. Это может включать проверку метаданных и использование цифровых подписей.

- Целостность. Данные должны быть защищены от несанкционированного доступа и изменений. Это может быть достигнуто с помощью шифрования и других методов защиты.

- Соответствие правовым нормам. Электронные доказательства должны быть собраны и представлены в соответствии с законодательством, именно для правильного изъятия таких носителей приглашается лицо, обладающее узкими знаниями в этой области - специалист.

- Релевантность. Данные должны быть непосредственно связаны с рассматриваемым делом и иметь доказательную ценность.

- Экспертная оценка: Полученная электронная информация часто требует участие эксперта для анализа и интерпретации электронных данных, чтобы подтвердить их достоверность и значимость.

Не стоит исключать и тот факт, что возможны также и некоторые проблемы при использовании электронных носителей информации в качестве доказательств:

- Электронные данные могут быть легко изменены или подделаны, что вызывает сомнения в их достоверности.

- Существует определенная необходимость в использовании специального оборудования и программного обеспечения для доступа и проверки данных.

- Также существует риск утечки или несанкционированного доступа к конфиденциальной информации.

Развивающиеся технологии: По мере развития технологий старые формы электронных носителей информации могут устареть, что потенциально делает хранящиеся данные недоступными. Это поднимает вопросы о сохранении цифровых доказательств с течением времени.

Следует отметить, что электронные носители информации стали незаменимыми источниками доказательств в современном обществе, служа динамичным и всеобъемлющим источником информации о событиях, взаимодействиях и транзакциях. Их значение в судебных разбирательствах, расследованиях и управлении информацией неоспоримо. Тем не менее, приемлемость электронных доказательств в суде зависит от различных факторов, включая актуальность, подлинность и соблюдение правовых стандартов и стандартов конфиденциальности. По мере дальнейшего развития цифрового пространства роль электронных носителей информации в юридической практике, цифровой криминалистике и управлении информацией будет продолжать расширяться. Разобраться в сложностях электронных доказательств - постоянная задача как для юристов, так и для судебных экспертов, а также специалистов в области кибербезопасности. Эта теоретическая часть обеспечивает основу для понимания важности и сложностей электронных носителей информации как источников доказательств в эпоху цифровых технологий, освещая их ключевую роль в поисках истины и справедливости.

2. Получение доказательственной информации на локальных и сетевых электронных носителях

Цифровая эпоха привела к смене парадигмы в том, как мы генерируем, храним и распространяем информацию. Электронные носители информации, включая локальные устройства хранения данных и онлайн-платформы, стали жизненно важными источниками доказательственной информации. В работе исследуются уникальные особенности и проблемы, связанные со сбором, проверкой и анализом цифровых доказательств. Мы углубляемся в методологии, юридические аспекты и новые технологии, лежащие в основе сложного процесса использования электронных носителей информации в следственных и юридических целях.

Электронные средства массовой информации, охватывающие множество цифровых платформ, таких как персональные компьютеры, смартфоны, социальные сети, облачные хранилища и многое другое, изменили ландшафт доказательственной информации. Огромный объем данных, генерируемых и хранящихся на электронных носителях, имеет серьезные последствия для расследований и судебных разбирательств. В этой статье рассматриваются отличительные особенности, которые определяют сбор, проверку и анализ доказательственной информации на электронных носителях, проливающие свет на вызовы и возможности, предоставляемые цифровой эпохой.

Сбор доказательственной информации

Сбор доказательственной информации с электронных носителей — это многогранный процесс, который включает в себя ряд определенных особенностей, которые в первую очередь зависят от типа носителя или устройства, с которого эта информация изымается.

Для сбора доказательственной информации с различных типов цифровых устройств можно использовать следующую схему:

1. Идентификация устройства. На этом этапе происходит выявление потенциальных источников цифровых доказательств. Это могут быть компьютеры, мобильные устройства, серверы, облачные хранилища и другие электронные носители информации.

1.1. Определение типа устройства (компьютер, смартфон, планшет, сервер и т.д.).

1.2. Фото- и видеофиксация.

1.3. Запись серийного номера, модели и других идентификационных данных.

2. Изоляция устройства.

2.1. Отключение устройства от сети для предотвращения удаленного доступа (режим полета).

2.2. Использование специальных контейнеров или экранирующих пакетов для защиты от беспроводных сигналов (клетка Фарадея).

3. Создание образа данных. Изъятие цифровых носителей осуществляется с соблюдением процессуальных норм, чтобы обеспечить сохранность данных и их пригодность в качестве доказательств. Копирование данных производится с использованием специализированного программного обеспечения, такого как FTK Imager, с применением блокировщиков записи для предотвращения изменения исходных данных

3.1. Использование специализированного программного обеспечения для создания точной копии данных устройства.

3.2. Проверка целостности образа с помощью хеш-сумм (MD5, SHA-1).

4. Анализ данных. На этом этапе проводится детальный анализ собранных данных. Используются различные методы и инструменты для восстановления удаленной информации, анализа файловых систем, поиска скрытых данных и выявления цифровых следов, которые могут быть полезны для расследования.

4.1. Извлечение и анализ файлов, журналов, сообщений, фотографий и других данных (необходимой цифровой информации).

4.2. Использование инструментов для восстановления удаленных данных. (Recuva).

5. Документирование процесса.

5.1. Подробное описание всех действий, выполненных при сборе данных.

5.2. Фиксация времени, места и участников процесса. Все действия по сбору и анализу цифровых доказательств должны быть тщательно задокументированы. Это может быть создание отчетов, протоколов и других документов, которые могут быть использованы в суде для подтверждения подлинности и целостности собранных данных.

6. Хранение доказательств.

6.1. Безопасное хранение оригинального устройства и созданного образа данных.

6.2. Использование защищенных хранилищ для предотвращения несанкционированного доступа.

7. Производство судебной экспертизы.

7.1. Назначение экспертизы для подтверждения подлинности и целостности данных.

7.2. Подготовка экспертного заключения для представления в суде.

На завершающем этапе собранные и проанализированные цифровые доказательства представляются в суде. Важно, чтобы они были представлены в понятной и доступной форме, с учетом всех юридических требований и норм.

Данная схема обобщает схожие процессы получения доказательственной информации с цифровых носителей, но стоит учитывать, что от

спецификации объекта исследования, некоторые ее элементы могут быть другими. Вышеуказанный алгоритм поможет обеспечить целостность и достоверность собранных доказательств, что важно для их использования в судебных разбирательствах.

Таким образом, сбор, проверка и анализ доказательственной информации на электронных носителях представляют собой сложный и динамичный процесс. Эксперты в области цифровой криминалистики и юристы-профессионалы должны ориентироваться в среде, характеризующейся цифровыми изображениями, неустойчивым сбором данных и правовыми стандартами. Сохранение целостности данных, соблюдение правовых стандартов и использование новейших технологий имеют важное значение для использования потенциала электронных носителей информации в следственных и юридических целях. Понимание уникальных особенностей и вызовов этого процесса имеет решающее значение для достижения справедливости и истины в эпоху цифровых технологий.

Проверка и анализ доказательственной информации на электронных носителях

Эпоха цифровых технологий привела к появлению огромного количества доказательной информации из электронных средств массовой информации, что создает как возможности, так и проблемы для проверки и анализа. В этой научной статье исследуются методологии, инструменты и лучшие практики, связанные с проверкой и анализом цифровых доказательств, собранных из различных электронных медиа-источников. Мы вникаем в тонкости обеспечения целостности и подлинности данных и извлечения ценной информации для судебных разбирательств и следственных практик. Понимание нюансов проверки и анализа имеет первостепенное значение для использования всего потенциала электронных носителей информации в стремлении к правосудию.

Электронные носители информации, включающие в себя широкий спектр устройств и платформ, стали основными источниками доказательственной информации в цифровую эпоху. Проверка и анализ этой информации являются ключевыми шагами в судебном разбирательстве, цифровой криминалистике и следственной практике. В этой статье рассматриваются проблемы и методологии проверки и анализа цифровых доказательств из различных электронных медиа-источников, проливается свет на методы и передовой опыт, лежащие в основе этих важнейших процессов.

Проверка играет ключевую роль в обработке доказательственной информации. Она включает в себя следующие этапы:

1. Проверка целостности данных.

- Использование хеш-сумм (например, MD5, SHA-1) для проверки, что данные не были изменены.

- Сравнение хеш-сумм оригинальных данных и их копий.

2. Аутентификация данных.

- Подтверждение подлинности данных с помощью цифровых подписей или сертификатов.

- Проверка метаданных файлов (дата создания, автор и т. д.).

3. Анализ логов и журналов.

- Изучение системных журналов для выявления подозрительных действий или изменений.

- Проверка журналов доступа для определения, кто и когда имел доступ к данным.

4. Восстановление удаленных данных.

- Использование специализированного ПО для восстановления удаленных или поврежденных файлов.

- Проверка восстановленных данных на предмет их целостности и подлинности.

5. Документирование процесса проверки.

- Подробная запись всех действий, выполненных при проверке данных.

- Фиксация результатов проверки и любых выявленных несоответствий.

6. Подготовка отчетов.

- Составление отчетов о результатах проверки для представления в суде или другим заинтересованным сторонам.

- Включение в отчеты всех доказательств и выводов, полученных в ходе проверки.

Проверка и анализ доказательственной информации на электронных носителях представляют собой сложные и динамичные процессы. Это требует сочетания технических знаний, юридических познаний и соблюдения этических норм. Понимание нюансов этих процессов необходимо следователям и юристам-профессионалам, чтобы в полной мере использовать потенциал электронных носителей информации в качестве источников доказательств в стремлении к правосудию и установлению истины в эпоху цифровых технологий. Справляясь с трудностями и перенимая лучшие практики, профессионалы могут эффективно проверять, анализировать и представлять электронные доказательства для судебных разбирательств и расследований.

Литература

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (в ред. от 14.07.2023) // Собр. законодательства РФ. 2001. 24 дек. № 52, ч. 1. Ст. 4921.
2. Афанасьев Е.В. Некоторые особенности использования современных технологий в ходе осмотра места происшествия // Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму: материалы III Всерос. науч.-практ. конф. Краснодар: Краснодарский университет МВД России, 2020. С. 21–25.
3. Баркалова Ю.М. Подготовка экспертов по производству компьютерных судебных экспертиз: метод. рекомендации. Воронеж: Воронежский институт МВД России, 2013. URL: <http://libkrumvd.ru>
4. Введенская О.Ю. Информационно-телекоммуникационная сеть Интернет как источник следовой информации о криминальном событии: фондовая лекция. Краснодар: Краснодарский университет МВД России, 2016. URL: <http://libkrumvd.ru>
5. Государственная автоматизированная система Российской Федерации «Правосудие». URL: <https://sudrf.ru> (дата обращения: 25.05.2023).
6. Еремченко В.И., Зиновьева Н.С., Алексеенко И.Л. Юридические и организационные аспекты использования информационно-телекоммуникационных систем в целях противодействия экстремистской деятельности в современных условиях: науч.-практ. пособие. Краснодар: Краснодарский университет МВД России, 2015.
7. Кузнецов А.А., Муленков Д.В., Пропастин С.В. и др. Тактика следственных действий, направленных на отыскание, обнаружение и исследование электронных носителей и информации на них: учеб. пособие. Омск: Омская академия МВД России, 2015.
8. Методы и способы получения доказательственной информации с электронных носителей: курс лекций / сост. А.В. Скачко. Краснодар: Краснодарский университет МВД России, 2014. URL: <http://libkrumvd.ru>
9. Официальный сайт МВД России. URL: <https://мвд.рф> (дата обращения: 25.05.2023).
10. Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru> (дата обращения: 25.05.2023).
11. Портал открытых данных России. URL: <https://data.gov.ru> (дата обращения: 25.05.2023).
12. Портал правовой статистики Генеральной прокуратуры Российской Федерации. URL: <http://crimestat.ru> (дата обращения: 25.05.2023).

Оглавление

Предисловие.....	3
1. Правовые основы доказательственной информации на электронных носителях.....	4
2. Получение доказательственной информации на локальных и сетевых электронных носителях.....	11
Литература.....	15

Учебное издание

Афанасьев Евгений Владимирович
Аругюнян Вадим Рафаэлевич
Бычкова Екатерина Сергеевна и др.

**ОСОБЕННОСТИ ПОЛУЧЕНИЯ
ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ
С ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ**

Методические рекомендации

В авторской редакции
Компьютерная верстка *С. В. Коноваловой*

ISBN 978-5-9266-2074-7



Подписано в печать 27.09.2024. Формат 60x84 1/16.
Усл. печ. л. 1,0. Тираж 60 экз. Заказ 280.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.