Научная статья
https://doi.org/10.24412/2220-2404-2025-9-31
УДК 343.98

Attribution
cc by

ПРИМЕНЕНИЕ ХЭШИРОВАНИЯ ДЛЯ ПОДТВЕРЖДЕНИЯ НЕИЗМЕННОСТИ ФАЙЛОВ ПРИ КОПИРОВАНИИ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ

Пономарев В.Е.
Кубанский государственный университет, https://orcid.org/0000-0002-1613-5749

Аннотация: *В статье рассматриваются вопросы применения хэш-функций для подтверждения неизменности электронной информации в процессе её копирования и использования в криминалистической практике. Обосновывается необходимость проверки тождественности оригинала и копии электронных данных, что особенно актуально при работе с большими объёмами информации и не мультимедийными файлами. Раскрывается алгоритм применения хэш-функций: вычисление хэш-суммы оригинала, создание копии и сравнение контрольных значений. Особое внимание уделяется достоинствам метода — детерминированности, компактности результата и невозможности восстановления исходных данных из хэш-значения. Отмечены также недостатки, в том числе вероятность коллизий и высокая чувствительность к изменениям исходного файла. Рассматриваются возможности применения «нечётких хэш-функций» как перспективного направления исследований. Предложен алгоритм действий следователя при копировании электронных доказательств с использованием как специализированных, так и штатных программных средств.*

Ключевые слова: *электронные доказательства, хэш-функция, хэш-сумма, копирование, криминалистика, неизменность данных, целостность информации, контрольная сумма, нечёткое хэширование.*

Финансирование: *инициативная работа.*

Original article

APPLICATION OF HASHING FOR CONFIRMING THE INTEGRITY OF FILES IN THE PROCESS OF COPYING ELECTRONIC EVIDENCE

Vitaly E. Ponomarev
Kuban State University

Abstract: *The article examines the use of hash functions to confirm the integrity of electronic information during its copying and application in forensic practice. It substantiates the necessity of verifying the identity of the original and the copied electronic data, which is particularly relevant when dealing with large volumes of information and non-multimedia files. The algorithm of applying hash functions is described: calculating the hash value of the original, creating a copy, and comparing control values. Special attention is given to the advantages of the method — determinism, compactness of the result, and the impossibility of restoring the original data from the hash value. The disadvantages are also noted, including the possibility of collisions and the high sensitivity to even minor file modifications. The potential of using "fuzzy hash functions" as a promising research direction is considered. An algorithm of investigator's actions for copying electronic evidence with the use of both specialized and standard software tools is proposed.*

Keywords: *electronic evidence, hash function, hash value, copying, forensic science, data integrity, information authenticity, checksum, collision, fuzzy hashing.*

Funding: *Independent work.*

Введение

В практике копирования электронной информации возникает важный и закономерный вопрос о том, как убедится в том, что полученная на иной носитель копия информационно соответствует оригиналу. Как следователю убедится, что процесс копирования прошел корректно и полученный в результате файл действительно содержит информацию, которая была на оригинальном носителе. Проблем не возникает, если файл небольшой и представляет собой мультимедиа, а значит проверку корректности копирования можно осуществить, просто воспроизведя файл, но если необходимо скопировать большой объем данных, либо файл не являются мультимедийными, то задача убедиться в совпадении оригинала и копии выходит на первый план.

Обсуждение

Копирование может выступать как обособленный от изъятия носителя способ (средство) получения доказательств, на основе данных, хранящихся на носителе электронной информации: в том случае, если принимается решение о копировании без изъятия самого носителя электронной информации. Причиной может быть, как принципиальная невозможность изъятия носителя (например, в случае, если в качестве носителя выступает удаленный сервер), так и просто в результате признание следователем изъятия носителя нецелесообразным в рамках конкретной следственной ситуации.

© Пономарев В.Е., 2025

Во-втором случае копирование применяется, как последующий этап закрепления электронных доказательств, применяемый к информации, которая хранится на изымаемом или ранее изъятом электронном носителе информации. В данных обстоятельствах копирование решает задачу не только закрепления электронной информации, но также одновременно и задачу извлечения такой информации с её оригинального носителя, перенос её на удобный для следователя носитель и придание этой информации такой формы, которую будет удобно использовать, при этом не подвергаясь риску утратить или повредить первоисточник. В том числе и в тех случаях, когда изъятый электронный носитель информации поврежден либо может быть поврежден в процессе хранения. В любом случае хранить информацию надежнее, чем хранить неизвестный носитель.

Скачивание файлов, из источников в сети Интернет или иной информационной сети (например, локальной сети) мы считаем частным случаем копирования, поскольку, в этом случае результатом копирование является получение файла, отличие только в пути, который проходит информация. Однако, в этом случае требуется дополнительно фиксация в протоколе откуда, в какое время и с использованием какого программного обеспечения был получен файл.

Хэширование может применятся, как в первом, так и во втором случае, но нами в рамках настоящей статьи рассматривается преимущественно первая ситуация.

Как установлено в Р 34.11–2012. «Информационная технология. Криптографическая защита информации. Функция хеширования», хэш-функция — это алгоритм, отображающий данные произвольной длины в битовую строку фиксированной длины (хэш-значение); в прикладных стандартах она используется, в том числе, для обеспечения целостности и аутентичности информации [1].

Вопрос использования в криминалистике хэш-функций поднимался неоднократно, как напрямую, так и с точки зрения смежных областей. Рассматривался также вопрос применения хэш-функций при копировании электронной информации для фиксации состояния компьютерной информации в конкретный момент времени и обеспечения возможности идентификации такой информации в дальнейшем [2, с.135]. Д.В. Овсянников описывает хэширование, как способ обеспечения целостности компьютерной информации с использованием специального программного обеспечения [3,с.18]. Ю.А. Бондаренко рассматривал вопрос о применении возможности использования данных хэш-функций при расследовании мошенничеств с использованием электронных подписей [4]. Необходимо также отметить предложения по использованию хэш-функция для удостоверения электронных доказательств при передачи на судебно-экспертное исследование [5, с.258].

Алгоритм работы хэш-функции следующий:

1. Алгоритм хэширования (например, SHA-256) принимает на вход данные любой длины.
2. Преобразует их в строку фиксированной длины (например, 64 символа для алгоритма SHA-256).
3. Результат всегда одинаков для одних и тех же входных данных. Даже минимальное изменение входных данных полностью меняет хэш.

У данного метода есть существенные достоинства, кроме того, что это единственный на сегодня надежный способ убедится в точном совпадении копии и «оригинала». Хэш детерминирован, то есть одни и те же данные будут давать один и тот же результат. Также результаты хэширования являются необратимыми, то есть по хэшу нельзя восстановить исходный файл (достаточно очевидно, что невозможно получить целый файл из множества бит всего из 64 символов). Достоинством получения хэш-суммы является то, что она позволяет любой объем данных зафиксировать в виде относительно небольшой последовательности символов, пригодной, в том числе, для занесения в бумажный протокол и дальнейшего сравнения с заново рассчитанной хэш-функции, что позволит убедиться в неизменности файла.

Ну и конечно, незаменимость применения хэш-функций состоит в том, что запись хэш суммы при копировании данных позволяет удостоверится в их неизменности на протяжении всего процесса расследования, может удостоверить неизменность путем сверки хэш сумм оригинала файла и его копии или сверки с хэш-суммой, занесенной в протокол следственного действия.

Есть также и недостатки: первый получил название «коллизия». Это проблема возникает, когда мы пытаемся свести бесконечное множество (набор данных всех потенциально существующих, существовавших и вероятно созданных в будущем файлов – бесконечен) к конечному множеству – число перестановок букв и цифр в хэш-сумме хоть и очень велико, но не бесконечно, поскольку хэш сумма имеет конечное число символов (например, 64 символа для алгоритма SHA-256). Это приводит к тому, что в теории может существовать два различных набора данных – два файла, каждый из которых содержит разный набор данных, но хэш суммы у них совпадают. Однако, на практике практически невозможно представить ситуацию, чтобы совпадению были подвержены два осмысленных набора данных. Кроме того, существует проблема поиска таких коллизий, решенная для алгоритма MD5, впоследствии признанным небезопасным и постепенно выведенным из использования [6].

Второй недостаток и одновременно достоинство хэш функций заключается в их точности. Поскольку на вход принимается набор данных, то изменения даже одного бита (одной единицы или одного нуля) информации в файле приводит к тому, что такой файл будет иметь другую хэш функцию.

Если мы хотим использовать данную конструкцию для удостоверения неизменности файлов, то

© Пономарев В.Е., 2025

необходимо учитывать, что любое, даже совершенно случайное или ненамеренное и незначительное изменение в файле, сделанное самим пользователем, либо произведенное в автоматическом режиме в результате работы какой-либо программы делает такой файл недопустимым доказательством. При этом с точки зрения пользователя, информация, содержащаяся в файле - не изменится.

В связи с этим не следует подходить к решению вопроса использования хэш-сумм комплексно, необходимо учитывать не только неизменность хэша, но и информационную составляющую. Оба критерия должны оцениваться вместе.

В качестве примера можно рассмотреть изображение, каждый отдельный пиксель которого закодирован цветом, определяемым тремя числами от 0 до 255 для 3 цветов – красного, зеленого и синего (система RGB), где число – интенсивность цвета для каждого отдельного пикселя. Для примера, визуально определить изменения интенсивности красного цвета с 41 до 42 на отдельном пикселе или даже группе пикселей никак не повлияет на воспринимаемое человеком изображение. Визуально определить такое изменение невозможно, но с точки зрения хэш функций это будет два разных файла.

Проблема может показаться несерьезной, когда идет сравнение между всего двумя файлами, однако, уже на сегодняшний день объемы данных могут быть большими и очень большими, что делает процедуру ручного сравнения «в лоб» не только очень затратными по временным и трудовым ресурсам, но просто невозможной при большом объеме данных.

Существуют технические решения проблемы идентификации схожих, но не идентичных файлов, одно из них – применение «нечетких хэш-функций». Они по своим свойствам аналогичны традиционным, то есть преобразуют массив данных в конечную строку определенной длины, однако нечёткая хэш-сумма действует наоборот, и, при незначительном изменении исходного файла, изменяет своё значение пропорционально объему изменений исходных данных [7, с.42]. Достигается это за счёт разбивки исходного файла на отдельные куски и применение хэш-функции к ним по отдельности, после чего на их основе высчитывается итоговый результат. Применение нечетких хэш-функций в криминалистике на сегодняшний день не рассматривалось, однако это перспективное направление исследований, которое может решить обозначенные проблемы.

Алгоритм применения хэш-функций в криминалистике основывается на необходимости подтверждения неизменности электронных доказательств в процессе их копирования.

Первоначально необходимо определить файл или электронный носитель, подлежащий копированию, закрепить в протоколе его основные признаки: дата и время осуществления копирования, сведения об устройстве, внешний вид, его состояние, серийные номера и иные идентифицирующие признаки электронного носителя информации или комплексного компьютерного устройства (ноутбука, персонального компьютера), с которого осуществляется копирование электронной информации.

Существует два варианта действий, если речь идет о внешнем или внутреннем носителе электронной информации (например, о Flash-накопителе, HDD и др.), то есть к устройству, не обладающему операционной системой, и значит возможности осуществить хэширование, в этом случае такой носитель необходимо подключить к устройству следователя или эксперта, как это описывает П.С. Пастухов [8].

Второй вариант, если информация находится в рамках комплексного компьютерного устройства (персонального компьютера, ноутбука, смартфона, видеорегистратора и тд.) либо на удаленном сервере в сети Интернет и извлечение носителя электронной информации для его самостоятельного подключения к устройству следователя. В этом случае возникает необходимость запуска программного обеспечения для вычисления хэш-суммы на самом исследуемом устройстве. В этом случае к этому устройству необходимо будет подключить носитель электронной информации, на который осуществляется копирование.

Второй случай сложнее, поскольку в этом случае программное обеспечение для вычисления хэш-суммы файлов, необходимо подбирать в зависимости от операционной системы исследуемого компьютера. На практике для фиксации контрольных сумм на самом исследуемом устройстве (когда извлечение носителя невозможно) можно использовать штатные, не специализированные средства, доступные на соответствующей операционной системе: в среде Windows — встроенную утилиту «certutil» для расчёта SHA-256, в средах Unix/Linux — стандартную команду «sha256sum», на компьютерах Apple — утилиту «shasum». Однако, могут применятся и специализированные криминалистические программы, например, можно привести FTK Imager [9], EnCase Forensic [10], X-Ways Forensics [11], отечественный комплекс Мобильный криминалист [12] и многие другие.

После получения хэш-суммы исходного файла необходимо осуществить копирование. Необходимо уточнить, что копирование может быть применено не только к отдельному файлу, но и, например, к каталогу (папке), содержащей множество файлов, а также и к условно «пустому» пространству носителя. Так, можно провести полное копирование и частичное копирование данных, содержащихся на электронном носителе информации. При частичном копировании создание копии происходит на уровне файловой системы - копируются отдельные файлы и каталоги (папки), содержащие отдельные файлы, при этом такое копирование выполняется штатными средствами операционной системы и не затрагивает пустое пространство носителя, а также поврежденные, частично или полностью удаленные файлы. Применение хэш-

© Пономарев В.Е., 2025

функции возможно, как при полном, так и при частичном копировании.

Частичное копирование применяется, если полное по какой-то причине невозможно или нецелесообразно, например, приходится осматривать работающую компьютерную систему, либо, с целью оперативного получения информации, размер носителя информации слишком большой [13, с.107].

При копировании информации с электронного носителя информации необходимо не допускать изменений информации на оригинальном носителе. Дело в том, что при подключении носителя электронной информации сама система может вольно или невольно вносить изменения в его содержание. Что бы этого избежать применяются специальные устройства на аппаратном уровне блокирующие внесение изменений в исходный носитель электронной информации. Примером таких устройств является Tableau Forensic Imager [14] или WiebeTech Forensic ComboDock [15].

После этого необходимо осуществить вычисление хэш-суммы файла-копии, расположенного на носителе электронной информации, на который производилось копирование. В случае, если полученные значения совпадают – можно сделать вывод о тождественности файлов.

Результаты

Вопрос подтверждения неизменности электронного файла при копировании может быть решен технически путем применения хэш-функции. Это уникальная строка символов фиксированной длины, которая генерируется из любых данных (текста, файла, изображения и т.д.) с помощью специального алгоритма. Хэш позволяет однозначно идентифицировать исходные данные и убедиться, что копия соответствует оригиналу. Хэш представляет собой число-буквенное значение, которое удобно фиксировать в протоколе следственного действия. Предлагается алгоритм копирования электронной информации, с использованием хэш-сумм файлов.

Заключение

Таким образом, для осуществления копирования необходимо наличие в распоряжении следователя переносного компьютерного устройства универсального назначения с операционной системой (ноутбук), позволяющего осуществлять подключение внешних устройств, аппаратные устройства для защиты от записи на подключаемых к нему устройствах, переходники для подключения различных технических устройств. Электронные носители информации, на которые осуществляется копирование, программное обеспечение, которое обеспечивает полное копирование электронной информации путем создания полного образа носителя, а также программное обеспечением для частичного копирования, обеспечивающим сохранение метаданных и фиксацию хэш-суммы (контрольной суммы).

Для копирования файлов с использованием хэш функций можно применять следующий алгоритм:

1) Определить файл или электронный носитель информации, подлежащий копированию;
2) Вычислить хэш-сумму оригинала с использованием специализированного ПО;
3) Создать побитовую копию (образ) носителя или копию файла;
4) Вычислить хэш-сумму копии тем же программным средством;
5) Сравнить хэш-суммы оригинала и копии;
6) Зафиксировать в протоколе алгоритм, программу и полученные значения хэш-сумм.

Таким образом, рекомендации по использованию хэш-функций должны также учитывать, что в некоторых случаях необходимо сравнивать не только полученные хэш-функции, но и сами файлы, в том случае, если такое сравнение возможно. Кроме того, своё применение могут найти «нечеткие хэш-функции».

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Список источников:

1. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хеширо-вания. М.: Стандартинформ, 2012. - СПС "Кодекс". URL: docs.cntd.ru/document/gost-r-34-11-2012 (дата обращения: 21.08.2025).

2. Гончар В.В. Галиев Д. В. Особенности осмотра и изъятия электронных носителей информации с учётом тре-бований ст. 164. 1 УПК РФ // Вестник Московского университета МВД России. 2020. №2. URL: https://cyberleninka.ru/article/n/osobennosti-osmotra-i-izyatiya-elektronnyh-nositeley-informatsii-s-uchyotom-trebovaniy-st-164-1-upk-rf (дата обращения: 11.02.2025).

3. Овсянников Д.В. Копирование электронной информации как средство уголовно-процессуального доказывания: автореф. дис. ... канд. юрид. наук. Саратов, 2016. EDN: OTAQYV

4. Бондаренко Ю.А. Особенности расследования мошенничества, совершенного с использованием электронной подписи // Гуманитарные, социально-экономические и общественные науки. 2020. №3. URL: https://cyberleninka.ru/article/n/osobennosti-rassledovaniya-moshennichestva-sovershennogo-s-ispolzovaniem-elektronnoy-podpisi (дата обращения: 11.02.2025). DOI: 10.23672/SAE.2020.2020.58143 EDN: QSDMWG

5. Шихалиева С.З. Отсутствие хэш-суммы как процессуальная ошибка, возникающая в судебной экспертизе при исследовании объектов в цифровой форме // Правовое государство: теория и практика. 2025. №1 (79). URL: https://cyberleninka.ru/article/n/otsutstvie-hesh-summy-kak-protsessualnaya-oshibka-voznikayuschaya-v-sudebnoy-ekspertize-pri-issledovanii-obektov-v-tsifrovoy-forme (дата обращения: 21.08.2025). DOI: 10.33184/pravgos-2025.1.28 EDN: BNTUWA

© Пономарев В.Е., 2025

6. Отчёт о расследовании SolarWinds: как злоумышленники обманули Microsoft и агенства США [Электронный ресурс] // Хабр. 28.07.2021. URL: https://habr.com/ru/articles/595013/ (дата обращения: 18.08.2025).

7. Тюрин К. А. Нечёткое хэширование в задачах информационной безопасности // Обзор.НЦПТИ. 2019. №1 (16). URL: https://cyberleninka.ru/article/n/nechyotkoe-heshirovanie-v-zadachah-informatsionnoy-bezopasnosti (дата обращения: 11.02.2025). EDN: PIGOEA

8. Пастухов П.С. Средства проверки надежности "электронных" доказательств в ходе производства по уголов-ному делу // Пробелы в российском законодательстве. 2015. №3. URL: https://cyberleninka.ru/article/n/sredstva-proverki-nadezhnosti-elektronnyh-dokazatelstv-v-hode-proizvodstva-po-ugolovnomu-delu (дата обращения: 21.08.2025). EDN: TYQCCB

9. FTK Imager: программа для ЭВМ [Электронный ресурс]. URL: https://www.exterro.com/ftk-product-downloads/ftk-imager-4-7-3-81 (дата обращения: 18.08.2025).

10. EnCase Forensic (OpenText): программа для ЭВМ [Электронный ресурс]. URL: https://www.opentext.com/products/forensic (дата обращения: 18.08.2025).

11. X-Ways Forensics (X-Ways Software Technology AG): программа для ЭВМ [Электронный ресурс]. URL: https://www.x-ways.net/forensics/ (дата обращения: 18.08.2025).

12. Мобильный Криминалист Эксперт Плюс" (МКО Системы): программа для ЭВМ [Электронный ресурс]. URL: https://mko-systems.ru/mobile-expert/ (дата обращения: 18.08.2025).

13. Россинская, Е. Р., Рядовский, И. А. Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика // Lex Russica. - 2021. - Т. 74, № 9. DOI: 10.17803/1729-5920.2021.178.9.102-118 EDN: WUUYUW

14. OpenText™ Tableau Forensic TX1 Imager: аппаратный криминалистический имиджер [Электронный ресурс]. URL: https://www.opentext.com/media/product-overview/opentext-forensic-tx1-imager-po-en.pdf (дата обращения: 18.08.2025).

15. WiebeTech Forensic ComboDock FCDv6 (CRU Data Security Group): док-станция с режимом write-blocking [Электронный ресурс]. URL: https://cdsg.com/products/forensic-write-blocking-drive-docks (дата обращения: 18.08.2025).

References

1. GOST R 34.11-2012. Information technology. Cryptographic protection of information. The hashing function. Moscow: Standartinform, 2012. - SPS "Codex". URL: docs.cntd.ru/document/gost-r-34-11-2012 (date of application: 08/21/2025).

2. Gonchar V.V. Galiev D. V. Features of inspection and seizure of electronic media, taking into account the requirements of art. 164.1 of the Criminal Procedure Code of the Russian Federation // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2020. No. 2. URL: https://cyberleninka.ru/article/n/osobennosti-osmotra-i-izyatiya-elektronnyh-nositeley-informatsii-s-uchyotom-trebovaniy-st-164-1-upk-rf (date of request: 02/11/2025).

3. Ovsyannikov D.V. Copying of electronic information as a means of criminal procedural proof: abstract of the dissertation. ... kand. jurid. sciences'. Saratov, 2016. EDN: OTAQYV

4. Bondarenko Yu.A. Features of the investigation of fraud committed using an electronic signature // Humanities, socio-economic and social sciences. 2020. No. 3. URL: https://cyberleninka.ru/article/n/osobennosti-rassledovaniya-moshennichestva-sovershennogo-s-ispolzovaniem-elektronnoy-podpisi (date of request: 02/11/2025). DOI: 10.23672/SAE.2020.2020.58143 EDN: QSDMWG

5. Shikhalieva S.Z. The absence of a hash sum as a procedural error that occurs in forensic examination when examining objects in digital form // The rule of law: theory and practice. 2025. No. 1 (79). URL: https://cyberleninka.ru/article/n/otsutstvie-hesh-summy-kak-protsessualnaya-oshibka-voznikayuschaya-v-sudebnoy-ekspertize-pri-issledovanii-obektov-v-tsifrovoy-forme (date of request: 08/21/2025). DOI: 10.33184/pravgos-2025.1.28 EDN: BNTUWA

6. SolarWinds Investigation Report: How hackers deceived Microsoft and US agencies [Electronic resource] // Habr. 07/28/2021. URL: https://habr.com/ru/articles/595013 / (date of access: 08/18/2025).

7. Tyurin K. A. Fuzzy hashing in information security tasks // Review.NCPTI. 2019. No. 1 (16). URL: https://cyberleninka.ru/article/n/nechyotkoe-heshirovanie-v-zadachah-informatsionnoy-bezopasnosti (date of request: 02/11/2025). EDN: PIGOEA

8. Pastukhov P.S. Means of verifying the reliability of "electronic" evidence in the course of criminal proceedings // Gaps in Russian legislation. 2015. No. 3. URL: https://cyberleninka.ru/article/n/sredstva-proverki-nadezhnosti-elektronnyh-dokazatelstv-v-hode-proizvodstva-po-ugolovnomu-delu (date of request: 08/21/2025). EDN: TYQCCB

9. FTK Imager: a computer program [Electronic resource]. URL: https://www.exterro.com/ftk-product-downloads/ftk-imager-4-7-3-81 (date of request: 08/18/2025).

10. EnCase Forensic (OpenText): a computer program [Electronic resource]. URL: https://www.opentext.com/products/forensic (date of access: 08/18/2025).

11. X-Ways Forensics (X-Ways Software Technology AG): computer program [Electronic resource]. URL: https://www.x-ways.net/forensics / (date of access: 08/18/2025).

12. Mobile Criminologist Expert Plus" (MKO Systems): computer program [Electronic resource]. URL: https://mko-systems.ru/mobile-expert / (date of access: 08/18/2025).

13. Rossinskaya, E. R., Ryadovsky, I. A. Tactics and technology of non-verbal investigative actions in cases of computer crimes: theory and practice // Lex Russica. - 2021. - Vol. 74, No. 9. DOI: 10.17803/1729-5920.2021.178.9.102-118 EDN: WUUYUW

14. OpenText Tableau Forensic TX1 Imager: hardware forensic imager [Electronic resource]. URL: https://www.opentext.com/media/product-overview/opentext-forensic-tx1-imager-po-en.pdf (date of request: 08/18/2025).

15. WiebeTech Forensic ComboDock FCDv6 (CRU Data Security Group): dock with write-blocking mode [Electronic resource]. URL: https://cdsg.com/products/forensic-write-blocking-drive-docks (date of request: 08/18/2025).

Информация об авторе:
Пономарев Виталий Евгеньевич, старший преподаватель кафедры криминалистики и правовой информатики Кубанский государственный университет, E-mail: 9529788272@mail.ru
Vitaly E. Ponomarev, Senior Lecturer at the Department of Criminology and Legal Informatics, Kuban State University

Статья поступила в редакцию / The article was submitted 22.08.2025;
Одобрена после рецензирования / Approved after reviewing 13.09.2025;
Принята к публикации / Accepted for publication 20.09.2025.
Автором окончательный вариант рукописи одобрен.

© Пономарев В.Е., 2025