Научная статья
УДК 343.98

КОПИРОВАНИЕ ЦИФРОВОЙ ИНФОРМАЦИИ С ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ: ДИСКУССИОННЫЕ ВОПРОСЫ СЛЕДСТВЕННОЙ И СУДЕБНОЙ ПРАКТИКИ

Сергей Леонидович Кисленко[1], Андрей Денисович Фокин[2]
[1,2]Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), г. Москва, Российская Федерация,
[1]ser- kislenko@yandex.ru
[2]adfokin@msal.ru

Аннотация. Традиционные способы совершения преступлений, предполагающие оставление материально-фиксированных следов и непосредственный контакт между преступником и жертвой, активно отходят на второй план, уступая место дистанционным и бесконтактным их разновидностям. Интеграция в различные сферы общественной жизни информационных технологий неизбежно повлекла применение таких технологий преступниками для модернизации способов криминальных деяний. В связи с этим правоохранительным органам приходится все чаще сталкиваться с необходимостью работы с цифровыми источниками информации. Однако правоприменители оказались не вполне готовыми к «цифровым» изменениям в общественной жизни. Осложняется это медленными осмыслениями «цифровизации» законодателем.

В статье рассматриваются особенности работы с носителями цифровой информации, а также специфика ее фиксации и изъятия. Раскрываются особенности содержания такой информации, соотношение терминов «копирование» и «клонирование» цифровой информации и значение указанных действий для назначения судебных экспертиз. Рассматривается отличие вышеуказанных действий и через призму разницы задач, стоящих перед следователем и экспертом.

Предлагается авторское определение копирования компьютерной информации. Освещается вопрос о допустимости скопированной информации для дальнейшего ее признания доказательством по уголовному делу.

Ключевые слова: расследование преступлений, криминалистическая техника, экспертиза, следственный осмотр, источник криминалистически значимой информации, копирование цифровой информации, допустимость доказательства.

Для цитирования: Кисленко С. Л., Фокин А. Д. Копирование цифровой информации с электронных носителей: дискуссионные вопросы следственной и судебной практики // Криминалистика: вчера, сегодня, завтра. 2026. Т. 38. № 2. С. 70–77.

COPYING DIGITAL INFORMATION FROM ELECTRONIC MEDIA: ISSUES OF INVESTIGATIVE AND JUDICIAL PRACTICE

Sergey L. Kislenko[1], Andrey D. Fokin[2]
Moscow State Law University named after O.E. Kutafin (MSLA), Moscow, Russian Federation
[1]ser- kislenko@yandex.ru,
[2]adfokin@msal.ru

Abstract. Traditional methods of committing crimes, which involve leaving material traces and direct contact between the perpetrator and the victim, are increasingly being replaced by remote and non-contact methods. The integration of information technology into various areas of public life has inevitably led to the use of such technology by criminals to modernize their methods of criminal activity. In this regard, law enforcement agencies are increasingly faced with the need to work with digital sources of information. However, law enforcement agencies have not fully prepared themselves for the "digital" changes in public life. This is further complicated by the slow pace of "digitalization" by lawmakers.

The article discusses the features of working with digital information carriers, as well as the specifics of its fixation and seizure. It reveals the features of the content of such information, the relationship between the terms "copying" and "cloning" of digital information, and the significance of these actions for the appointment of forensic examinations. The article examines the difference between the above-mentioned actions through the lens of the tasks faced by the investigator and the expert.

The author proposes a definition of copying computer information. The article also addresses the issue of the admissibility of copied information as evidence in a criminal case.

Keywords: crime investigation, forensic techniques, expertise, investigative examination, source of forensic information, copying of digital information, admissibility of evidence.

For citation: Kislenko S. L., Fokin A. D. Kopirovaniye tsifrovoy informatsii s elektronnykh nositeley: diskussionnyye voprosy sledstvennoy i sudebnoy praktiki [Copying digital information from electronic media: issues of investigative and judicial practice]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2026, vol. 38. no. 2, pp. 70–77 (in Russ.).

Исследование выполнено в рамках программы стратегического академического лидерства «Приоритет-2030» (Центр компетенций «Киберправо»).

The study was conducted as part of the Priority-2030 Strategic Academic Leadership Program (Cyberlaw Competence Center).

Введение

Современные особенности электронных носителей информации предопределяют специфику криминалистических средств, приемов и методик, направленных на извлечение, исследование и фиксацию данной информации. Работа с такими объектами предусматривает не только учет процессуальной формы при оперировании с ними, но и закономерностей функционирования, как самих устройств, так и заключенной в них информации. Такая информация в большинстве своем имеет цифровую природу и представлена в виде сведений (сообщений, данных), представленных в виде электрических сигналов, независимо от средств их хранения, обработки и передачи (Примечание 1 к ст. 272 УК РФ). При этом данные сведения могут находиться в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах либо на любых внешних электронных носителях (дисках-накопителях, флеш-картах и т. п.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи. Представляется, что данное законодательное определение цифровой (компьютерной) информации формировалось на базе ее природы и характеристик.

Основная часть

Обобщение работ по данному вопросу позволяет выделить следующие специфические характеристики цифровой информации, учет которых необходим при выборе оптимальных приемов и средств, направленных на ее обнаружение, фиксацию, изъятие и исследование: ее обезличенность (между информацией и лицом, которое ее создает и использует, нет прямой связи) [1, с. 275]; опосредованность через материальный (электронный) носитель (изменяться, копироваться, применяться и использоваться только с помощью ЭВМ при наличии соответствующих устройств для ее ввода, чтения, записи, передачи) [2, с. 42]; возможность передачи по телекоммуникационным каналам связи компьютерных сетей; постоянное изменение в ходе работы с информацией пользователя и выполнения различных операций [3, с. 114]; возможность трансформации объема (сжатие и последующее восстановление); наличие индивидуализирующих признаков (метаданных)[1]; пригодность для автоматической обработки (поиска, удаления, восстановления и др.) и прочее. Данная специфика, как отмечается в литературе, предопределяет методологию формирования криминалистических приемов и средств проведения следственных действий, в рамках которой приоритет отводится кибернетическим методам, позволяющим осуществлять автоматический поиск и обработку информации, методам компьютерного моделирования, средствам цифро-аналогового преобразования полученной информации и пр.[2]

Также особенности носителей цифровой информации обусловливают последовательность действий

---

[1] Гаврилин Ю. В. Организационно-методическое обеспечение расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации // Деятельность органов внутренних дел по борьбе с преступлениями, совершенных с использованием информационно-телекоммуникационных технологий: учеб. пособие. М.: Изд-во Академии управления МВД России, 2019. С. 74.

[2] Смушкин А. Б. Цифровизация криминалистической деятельности + еПриложение: дополнительные материалы: учебное пособие. М.: КНОРУС, 2024. С. 155 – 156.

при работе с ними. Так, к числу первоочередных тактических задач при осмотре стационарного компьютера относится фиксация информации из его оперативной памяти, получение электронного образа содержимого жестких дисков, а также фиксация активных сетевых соединений[3].

Специфика электронных носителей информации, как источников доказательственной информации, предопределяет при работе с такими носителями особенности задействования специальных знаний, предусматривающих не только полное и точное получение информации, но и минимизацию потерь с учетом ее природы. В связи с этим справедливо отмечается в литературе, что лицо, осуществляющее первоначальный доступ к обследуемому объекту (электронному носителю информации), должно иметь соответствующую квалификацию, осознавать суть основных процессов, происходящих в компьютерной системе, и, соответственно, понимать физические принципы записи, хранения и удаления информации на каждом из носителей. Игнорирование данных положений может привести на практике к рискам неполного изъятия, уничтожения (например, при отсутствии паролей доступа к устройству) или подмены информации на электронных носителях, а также к неверной интерпретации ее характеристик (например, получена ли информация непосредственно из сети Интернет или из кэша).

Копирование является неотъемлемым свойством цифровой информации и связано с ее переносом на иные физические носители или в их пределах без изменения содержания. Однако технологическая составляющая данного процесса различается в зависимости от методов и целей переноса информации и напрямую влияет на понимание категории «неизменность переносимой информации». Если обратиться к уголовно-процессуальному законодательству, то анализ УПК РФ позволяет сделать вывод, что информация с изымаемых электронных носителей копируется (ч. 3 ст. 164.1 УПК РФ). При этом законодатель исходит из того, что при копировании информации должны обеспечиваться условия, исключающие возможность ее утраты или изменения (ч. 2.1. ст. 83 УПК РФ). А само копирование представлено в виде переноса информации на другой электронный носитель при сохранении неизменности первоначальной информации[4]. Что понимается под сохранением неизменности информации, законодатель не разъясняет. Отчасти это объясняется тем, что уголовно-процессуальное доказывание оказалось не вполне готовым к «электронным» изменениям в общественной жизни. Поэтому, как отмечается в литературе, в настоящее время можно констатировать стадию осмысления и теоретического обоснования некоторых цифровых и технических категорий со стороны законодателя [4, с. 33–34].

На наш взгляд, положение о сохранении неизменности копируемой

[3] Организация противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий: учебник : в 2 ч. / Гаврилин Ю. В., Пинкевич Т. В., Мартыненко Н. Э. [и др.]; под общ. ред. Ю. В. Гаврилина. М.: Академия управления МВД России, 2024. Ч. 1. С. 216.

[4] Постановление Пленума Верховного Суда РФ от 15.12.2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» // Российская газета от 28.12.2022. № 294.

информации следует рассматривать в контексте ее пригодности для дальнейшего использования в уголовном судопроизводстве. Однако обеспечение данного предписания не всегда коррелируется на практике с техническими аспектами копирования цифровой информации. Кроме того, отмечается разное понимание «неизменности» информации участниками уголовного судопроизводства. Так, для следователя перенос информации в неизменном виде необходим для обеспечения легитимности ее доказательственного значения, а для эксперта – для решения отдельных вопросов в рамках ее исследования.

В информатике различают разные способы переноса содержания цифровой информации. Так, копирование – это базовая операция, которая просто создает новую копию объекта, побитово копируя его содержимое. Клонирование, в свою очередь, представляет собой более сложный процесс, который, помимо создания копии, может включать в себя глубокое копирование вложенных объектов и структур данных. Клонирование позволяет создать точную копию текущего устройства, включая все приложения, настройки и файлы. Это полезно, если есть опасения потери важных данных из-за случайного удаления, неисправности устройства или сбоя системы. Например, при клонировании USB-накопителя, помимо данных, переносятся главная загрузочная запись диска и таблицы разделов. В результате клонирования получается готовый образ, который состоит из всех видимых и скрытых файлов и неиспользуемого пространства диска.

Понятно, что для следователя перенос скрытых файлов не столь необходим для обеспечения допустимости получаемого доказательства. И процессуально данная технология никак не влияет на процесс сохранения содержимого информации на принимаемом носителе в том виде, который необходим следователю для решения его задач. Однако дело меняется, когда речь заходит о проведении отдельных исследований такой информации в рамках компьютерно-технической экспертизы. В данных ситуациях перенос скрытых файлов может иметь существенное значение. Например, при решении вопросов об установлении обстоятельств создания и использования файлов и баз данных. На цифровом уровне файл содержит не только данные, которые поместил в него пользователь, но и целый ряд специфических атрибутов, благодаря которым система распознает данный пакет информации и размещает его в хранилище данных. Для извлечения некоторых характеристик файлов или баз данных требуется владение особыми навыками в сфере компьютерной информации, а также применение специальных современных технологий и, соответственно, оборудования. В данном случае эксперт прибегает именно к методу клонирования, то есть создаёт файл-образ жёсткого диска на своём компьютере, либо через специальное программное обеспечение посекторно копирует на другой жёсткий диск. Отчасти такая методика продиктована требованием законодательства о запрете эксперту совершать действия, которые могут привести к изменению основных свойств исследуемого объекта[5]. В некоторых ситуациях это продиктовано задачами экспертного исследования. Так, при проведении некоторых компьютерно-технических экспертиз по-

[5] Ст. 16 Федерального закона от 31.05.2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» // Собрание законодательства Российской Федерации от 4.06.2001 г. № 23 ст. 2291.

рой требуется создать точную копию исследуемого устройства памяти в целях сохранения доказательства противоправной деятельности; при этом носитель-копия должен в точности соответствовать оригиналу, включая физическую геометрию исправных и поврежденных секторов. Представляется, что именно клонирование позволяет обеспечить полноту сохранения свойств переносимой информации на специально выделенные экспертом зоны на тестовом компьютере (так называемое создание образа исследуемого носителя цифровой информации). В последующем именно над «образом» эксперт и осуществляет исследование.

Для того чтобы такой образ являлся эквивалентом оригинала, он должен представлять собой абсолютную копию исходных данных. Следовательно, каждый бит оригинала должен быть скопирован на такой образ. Для этого эксперты прибегают к различным методам клонирования носителей информации: клонирование с диска на диск в DOS; клонирование данных по сети [5, с. 58]. При этом такие действия эксперта должны проводиться только с использованием специализированного программного обеспечения, применение которого в исследовании должно быть обосновано и отражено в экспертном заключении [6, с. 113]. В частности, для копирования данных с мобильного телефона как при его осмотре, так и в ходе компьютерно-технической экспертизы используются специализированные программные средства (например, UFED Cellebrite, Oxygen Forensic Detective и пр.), которые обеспечивают извлечение информации на физическом уровне; логическое извлечение; извлечение файловой системы.

Выводы и заключение

Таким образом, современное понимание процесса копирования цифровой информации и правоприменительная практика его реализации предполагает учет его технических сторон в целях обеспечения эффективного решения задач уголовного судопроизводства разными его участниками (следователями, специалистами, экспертами). На наш взгляд, под копированием компьютерной информации следует понимать *перенос всех данных имеющейся информации на другой электронный носитель или создание файл-образа такой информации на другом носителе с помощью аппаратных или программных методов при сохранении неизменной первоначальной информации.*

Еще один немаловажный аспект, связанный с копированием цифровой информации – это обеспечение ее допустимости. Законодатель, предоставив право следователю на копирование такой информации с одного электронного носителя на другой, не установил перечень технических средств, которые могут быть задействованы в данном процессе (ч. 3 ст. 164.1 УПК РФ). Это вполне закономерно, поскольку угнаться за техническим прогрессом в данном вопросе представляется затруднительным. Однако ключевые положения применения технических средств, задействованные в копировании цифровой информации, должны быть закреплены на законодательном уровне. В первую очередь это касается вопроса сертификации используемого оборудования и программного комплекса. Это позволит избежать проблем, связанных с признанием недопустимой для использования в качестве доказательственной, полученной с их помощью цифровой криминалистически значимой информации [7, с. 27]. И самое главное – позволит минимизировать риски утери, искажения или иных инцидентов безопасности скопированной информации.

СПИСОК ИСТОЧНИКОВ

1. *Зиннуров, Ф. К., Хайруллова Э. Т.* Особенности работы с электронными носителями как источниками доказательств при проведении следственных действий // Вестник Казанского юридического института МВД России. 2018. № 2. С. 274 – 278.

2. Вехов, В. Б. Электронная криминалистика: понятие и система // Криминалистика: актуальные вопросы теории и практики: матер. междунар. науч.-практ. конф. – Ростов н/Д: Изд-во Ростовский юридический институт МВД РФ. 2017. С. *40 – 46.*

3. *Россинская, Е. Р.* Концепция частной криминалистической теории «информационно-компьютерное обеспечение криминалистической деятельности» // Деятельность правоохранительных органов в современных условиях: сбор. Матер. XXIII Междунар. науч.-практ. конф. – Иркутск: Изд-во Восточно-Сибирского ин-та МВД РФ, 2018. С. 113 – 118.

4. *Григорьев, В. Н., Максимов О. А.* Понятие электронных носителей информации в уголовном судопроизводстве // Вестник Уфимского юридического института МВД России. 2019. № 2. С. 33 – 44.

5. *Смолина, А. Р.* Методическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы: дис. … канд. технич. наук. Томск, 2017. 132 с.

6. *Зазулин, А. И.* Участие специалиста и производство судебных экспертиз при исследовании компьютерной информации // Правопорядок: история, теория, практика. 2018. № 1. С. 110 – 114.

7. *Черданцев, А. Ю.* Практические проблемы получения, анализа и последующей правильной интерпретации полученной цифровой криминалистически значимой информации // Эксперт-криминалист. 2022. № 4. С. 26 – 29.

REFERENCES

1. *Zinnurov, F. K., Khairullova E. T.* Osobennosti raboty s elektronnymi nositelyami kak istochnikami dokazatel'stv pri provedenii sledstvennykh deystviy [Features of working with electronic media as sources of evidence during investigative actions]. Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii – Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of the Russian Federation. 2018. no. 2. pp. 274–278. (in Russian).

2. *Vekhov, V. B.* Elektronnaya kriminalistika: ponyatiye i sistema [Electronic forensics: concept and system]. Kriminalistika: aktual'nyye voprosy teorii i praktiki: mater. mezhdunar. nauch.-prakt. konf. – Forensic science: current issues of theory and practice: proc. int. scientific and practical. conf. – Rostov n / D: Publishing house Rostov Law Institute of the Ministry of Internal Affairs of the Russian Federation. 2017. pp. 40–46. (in Russian).

3. *Rossinskaya, E. R.* Kontseptsiya chastnoy kriminalisticheskoy teorii «informatsionno-komp'yuternoye obespecheniye kriminalisticheskoy deyatel'nosti» [The concept of a private forensic theory “information and computer support for forensic activity”]. Deyatel'nost' pravookhranitel'nykh organov v sovremennykh usloviyakh: sbor. Mater. XXIII Mezhdunar. nauch.-prakt. konf. – Activities of law enforcement agencies in modern conditions: collection. Proc. XXIII Int. scientific and practical. conf. – Irkutsk: Publishing house of the East Siberian Institute of the Ministry of Internal Affairs of the Russian Federation, 2018. pp. 113–118. (in Russian).

4. *Grigoriev, V. N., Maksimov, O. A.* Ponyatiye elektronnykh nositeley informatsii v ugolovnom sudoproizvodstve [The concept of electronic storage media in criminal proceedings]. Vestnik Ufimskogo yuridicheskogo instituta MVD Rossii – Bulletin of the Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2019. No. 2. pp. 33–44. (in Russian).

5. *Smolina, A. R.* Metodicheskoye i algoritmicheskoye obespecheniye proizvodstva komp'yuterno-tekhnicheskoy ekspertizy: dis. … kand. tekhnich. nauk. [Methodological and algorithmic support for the production of computer-technical examination: diss. … Cand. of Technical Sciences]. Tomsk, 2017. 132 p. (in Russian).

6. *Zazulin, A. I.* Uchastiye spetsialista i proizvodstvo sudebnykh ekspertiz pri issledovanii komp'yuternoy informatsii [Participation of a specialist and the production of forensic examinations in the study of computer information]. Pravoporyadok: istoriya, teoriya, praktika. – Law and Order: History, Theory, Practice. 2018. No. 1. Pp. 110–114. (in Russian).

7. *Cherdantsev, A. Yu.* Prakticheskiye problemy polucheniya, analiza i posleduyushchey pravil'noy interpretatsii poluchennoy tsifrovoy kriminalisticheski znachimoy informatsii [Practical problems of obtaining, analyzing, and subsequently correctly interpreting the obtained digital forensically significant information] // Ekspert-kriminalist. – Forensic Expert. 2022. No. 4. Pp. 26–29. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Кисленко Сергей Леонидович, доктор юридических наук, доцент, профессор кафедры криминалистики. Московскоий государственный юридический университет имени О. Е. Кутафина (МГЮА). 125993, Российская Федерация, г. Москва, ул. Садовая-Кудринская, д. 9, стр. 2

Фокин Андрей Денисович, кандидат юридических наук преподаватель кафедры криминалистики. Московский государственный юридический университет имени О. Е. Кутафина (МГЮА). 125993, Российская Федерация, г. Москва, ул. Садовая-Кудринская, д. 9, стр. 2

INFORMATION ABOUT THE AUTHORS

Sergey L. Kislenko, Doctor of Law, Associate Professor, Professor, Department of Forensic Science, Kutafin Moscow State Law University (MSAL). 9, Bldg. 2, Moscow, Russian Federation, 125993.

Andrey Denisovich Fokin, PhD in Law, Lecturer of the Department of Forensic Science. Kutafin Moscow State Law University (MSAL). 9, Bldg. 2, Moscow, Russian Federation, 125993.