

В диссертационный совет
24.2.320.07, созданный на базе
федерального государственного
бюджетного образовательного
учреждения высшего образования
«Кубанский государственный
университет»

ОТЗЫВ

официального оппонента на диссертационное исследование
Пономарева Виталия Евгеньевича
на тему «Технико-криминалистическое обеспечение выявления и
закрепления электронных доказательств»,
представленное на соискание ученой степени
кандидата юридических наук
по специальности 5.1.4. Уголовно-правовые науки (Юридические науки)

Глобальные процессы цифровизации, затрагивающие все аспекты жизни человека и общества, в числе прочего создают колоссальное количество ситуаций, когда преступление, согласно известному принципу Локара, оставляет не только классические, но и цифровые следы. Несмотря на уже вполне достойный опыт научных и практических исследований этого феномена, как в науке, так и на практике сохраняется проблемное поле в действиях по обнаружению, фиксации и изъятию цифровых следов и преобразованию их в электронные доказательства при сохранении непрерывности содержащейся в них информации.

На решение этой проблемы и ориентирована рецензируемая диссертация. В ней достаточно детально и комплексно исследуются проблемы и закономерности технико-криминалистического обеспечения выявления и закрепления электронных доказательств в условиях цифровизации современного общества. **Тема исследования является безусловно актуальной** и не вызывающей сомнений в силу своей повышенной практической значимости и неполноты научной разработанности.

Соискатель корректно определил **объект и предмет** своего диссертационного исследования. Объектом исследования заявлены общественные отношения, возникающие в связи с совершением и расследованием преступлений, связанных с созданием, передачей, хранением и (или) использованием электронной информации. Предметом исследования выступают закономерности возникновения электронной информации о преступлении и его участниках, выявления и закрепления электронных доказательств, и основанные на этих закономерностях специальные средства и методы раскрытия и расследования преступлений. Таким образом, можно сделать вывод о том, что объект и предмет исследования сформулированы верно и входят в содержание научной специальности 5.1.4 – Уголовно-правовые науки (юридические науки), располагаясь на пересечении наук криминалистики и уголовного процесса.

Основная цель диссертации определена как получение нового научного знания, способствующего эффективному технико-криминалистическому обеспечению выявления и закрепления электронных доказательств; разработка и усовершенствование методов закрепления электронных доказательств.

Для достижения этой цели В. Е. Пономарёв поставил и успешно разрешил следующие **задачи**:

- определить понятие технико-криминалистического обеспечения выявления и закрепления электронных доказательств;
- классифицировать технико-криминалистические средства и методы по характеру воздействия на исследуемый объект;
- дифференцировать свойства электронной информации, отличающие её от иных видов информации;
- рекомендовать методы преодоления фальсификаций электронных доказательств с использованием систем искусственного интеллекта;
- определить сущность и дать понятие источника электронной информации;
- классифицировать электронные носители информации в зависимости от необходимости привлечения специалиста для их изъятия;
- разработать алгоритм получения электронной информации;
- разработать алгоритм действий следователя, обеспечивающий достоверность при копировании электронной информации;
- предложить внедрение в криминалистическую практику современных аппаратно-программных комплексов, обеспечивающих новые производные методы закрепления электронных доказательств.

Анализ текста представленной диссертации, а также автореферата и основных публикаций В. Е. Пономарёва даёт возможность сделать вывод о том, что формулировки цели и задач диссертационного исследования являются корректными и обоснованными, а сама **цель – достигнутой** в результате предпринятого исследовательского процесса.

Научная новизна диссертационного исследования не вызывает сомнений и определяется **существенным вкладом автора** в обозначенную тематику. Соискателем учёной степени получено новое знание, касающееся технико-криминалистического закрепления электронных доказательств: сформулировано понятие технико-криминалистического обеспечения выявления и закрепления электронных доказательств, дано понятие источника электронной информации, предложена классификация носителей электронной информации и файлов, разработаны и обоснованы подходы к применению производных методов закрепления доказательственной информации, позволяющие повысить полноту получаемых данных, разработана методика использования хэш-функций при копировании и хранении файлов, предложено использование современных аппаратно-программных комплексов, обеспечивающих новые производные методы закрепления электронных доказательств.

Сформулированные диссертантом **положения, выносимые на защиту, отвечают критерию научной новизны.**

Теоретическая значимость исследования заключается в уточнении современных научных представлений о технико-криминалистическом обеспечении выявления и закрепления электронных доказательств. В ходе работы были определены свойства электронной информации, предложена классификация её носителей и файлов, а также исследованы аппаратные, программные и аппаратно-программные средства, используемые в процессе выявления и закрепления электронных доказательств.

Теоретические положения, представленные в данном диссертационном исследовании, направлены на углубление и развитие общей теории доказательств и криминалистической науки.

Практическая значимость исследования состоит в том, что представленные положения могут быть использованы при подготовке следователей и дознавателей, в образовательном процессе, создании методических рекомендаций по технико-криминалистическому обеспечению деятельности по выявлению и закреплению электронных доказательств в электронной среде, а также могут быть использованы в практической работе органов предварительного следствия и дознания.

Эмпирическую базу исследования также видится достаточной и включает изучение 121 уголовного дела (к сожалению, часть из них – в форме приговоров), а также анкетирование 156 следователей и дознавателей.

Таким образом, **обоснованность, достоверность и репрезентативность** полученных диссертантом результатов, сделанных им выводов и вносимых предложений достаточно высокая.

Результаты диссертации апробированы при обсуждении на кафедре криминалистики и правовой информатики юридического факультета им. А. А. Хмырова ФГБОУ ВО «Кубанский государственный университет».

Результаты диссертации В. Е. Пономарёва также были должным образом апробированы в 12 научных статьях автора, 7 из которых опубликованы в изданиях, рекомендованных ВАК при Министерстве науки и высшего образования РФ для публикации основных научных результатов диссертаций, а также в докладах на 7 научных конференциях. Отдельные результаты внедрены в деятельность следственного управления Следственного Комитета Российской Федерации по Краснодарскому краю, Управления организации дознания ГУ МВД России по Краснодарскому краю, ФГБОУ ВО «Кубанский государственный аграрный университет» им. И Т. Трубилина, Краснодарского университета МВД России, ФГБОУ ВО «Кубанский государственный университет».

Таким образом, **апробацию диссертационного исследования следует считать достаточной.**

Диссертация состоит из введения, трех глав, включающих девять параграфов, заключения, списка использованных источников, приложений. Общий объём работы составляет 200 страниц. Структура исследования логична, последовательна и соответствует требованиям ВАК Российской Федерации.

Во **введении** обоснована актуальность темы исследования, степень научной разработанности темы, определены цель, задачи, объект и предмет, обозначены методология и методы исследования, теоретическая основа и нормативная база диссертации, эмпирическая основа исследования, научная новизна диссертации, сформулированы основные положения, выносимые на защиту, отмечены теоретическая и практическая значимость полученных результатов исследования, указаны достоверность и обоснованность результатов диссертации, приведены сведения об их апробации и внедрении, структура диссертации (с. 3–18).

Первая глава – «Теоретические основы технико-криминалистического обеспечения выявления и закрепления электронных доказательств» состоит из трёх параграфов (с. 19–63).

В первом параграфе – «Понятие технико-криминалистического обеспечения выявления и закрепления электронных доказательств» – исследуются существующие подходы к понятию технико-криминалистического обеспечения, анализируются критерии отнесения технических средств к системе технико-криминалистического обеспечения, в том числе их классификация и субъектный состав.

Во втором параграфе – «Информационная природа электронных доказательств» – изучается сущность и генезис понятия «информация» и «электронное доказательство», определяются составные аспекты понятия «электронное доказательство».

В третьем параграфе – «Влияние нейросетей и систем искусственного интеллекта на выявление и закрепление электронных доказательств» – анализируется влияние искусственного интеллекта на процесс выявления и закрепления электронных доказательств. Автор отмечает, что широкое распространение систем машинного обучения, искусственных нейросетей и программ на их основе существенно усложнило задачу работы с электронными доказательствами. При этом подчеркивается, что интерес к искусственному интеллекту проявляют не только криминалисты, но и преступники, в связи с чем на проблему можно взглянуть с двух сторон: как перспективный инструмент для криминалистики и как источник новых угроз для достоверности электронных доказательств.

Вторая глава – «Источники электронной информации и методы получения электронных доказательств» – рассматривает понятие «источник электронной информации», а также классификацию носителей, файлов и основные методы получения электронных доказательств (с. 64–104).

В первом параграфе – «Понятие и сущность источников электронной информации» – соискатель рассматривает сущность электронного носителя как основы для существования электронной информации, при этом разграничиваются понятия «электронный носитель информации», «источник электронной информации» и «файл». Особое внимание уделено доктринальным подходам к определению электронного носителя информации. Анализируется специфика носителей в составе сложных технических устройств. Большое внимание уделено понятию файла как минимальной единицы хранения электронной информации. Указывается, что файл имеет

определенную структуру, может быть идентифицирован по имени, расширению и метаданным, а для подтверждения его неизменности используется хэш-сумма.

Во втором параграфе второй главы – «Классификация источников электронной информации» – носители электронной информации разделяются на классы по критерию необходимости участия специалиста и группы – в зависимости от технических особенностей устройства. Представленная классификация может лечь в основу изменений порядка привлечения специалиста для изъятия электронных носителей информации, предусмотренных в рамках действующего процессуального законодательства.

В третьем параграфе – «Методы получения криминалистически значимой информации из электронных источников» – подчеркивается, что простое нахождение электронного носителя или источника информации не означает выявление доказательства, так как сведения, содержащиеся в них, требуют специального выделения и перевода в форму, пригодную для использования в расследовании. Важно не только обнаружить источник электронной информации, но и выявить среди содержащихся в нём данных именно криминалистически значимую информацию, после чего закрепить её в форме, пригодной для использования в процессе доказывания. Важным достижением этого раздела диссертации является алгоритм применения методов получения электронной информации.

Третья глава – «Технико-криминалистическое обеспечение выявления и закрепления электронных доказательств» – содержит знание о методах и технических средствах, применяемых в процессе выявления и закрепления электронных доказательств.

Первый параграф – «Технико-криминалистическое обеспечение изъятия электронных носителей информации» – посвящен роли таких носителей в процессе расследования и порядку их обнаружения и изъятия. В нём выделяются основные задачи технико-криминалистического обеспечения: выявление (обнаружение) носителей электронной информации, определение их вида и типа, описание в протоколе следственного действия и упаковка. Подробно рассматриваются вопросы изъятия устройств во включённом и выключенном состоянии.

Второй параграф «Технико-криминалистическое обеспечение копирования электронных доказательств» рассматривает возможность копирования электронной информации как метода сохранения электронных доказательств. Обозначены ряд проблем копирования электронной информации, предложен алгоритм действий следователя при копировании электронной информации с использованием хэш-суммы (контрольной суммы) файла с целью обеспечения неизменности электронного доказательства. Разграничиваются частичное и полное копирование электронной информации.

Третий параграф третьей главы «Производные способы закрепления электронной информации» посвящен рассмотрению методов, которые позволяют сохранить сведения без изъятия носителя электронной информации или её копирования. Суть производных способов состоит в сохранении информации в виде скриншотов (снимков экрана), скринкастов (видеозаписей

экрана), репродукционной фотосъёмки (видеозаписи) экрана устройства или прямого захвата видеосигнала. Эти методы не дают полного объёма информации, но более оперативны, обеспечивают меньший уровень вмешательства, что особенно важно, когда существует риск утраты сведений.

В **заключении** обобщены результаты проведённого исследования и акцентировано внимание на ключевых положениях работы.

В **приложениях** к диссертации представлены анкета-интервью для практических работников, результаты обобщения анкетирования практических работников, результаты изучения уголовных дел.

Соотнося поставленную цель и задачи исследования с достигнутыми результатами, отмечаем, что структура представленной работы раскрывает как тему диссертации в целом, так и основные её вопросы в логической последовательности, **работа является завершённым научно-квалификационным трудом монографического характера.**

Однако диссертация В. Е. Пономарёва, равно как и любая работа, раздвигающая границы научного знания, не лишена отдельных недостатков, в целом не снижающих общее впечатление о ней. Позволим себе высказать ряд замечаний, обусловленных этим феноменом.

1. В положении 1, выносимом на защиту, указано, что в систему технико-криминалистического обеспечения входят технические средства, программное обеспечение, аппаратно-программные комплексы, методы и приёмы выявления и закрепления электронных доказательств. Далее в этом же положении указывается, что в эту систему входят программное обеспечение и аппаратно-программные комплексы (технические средства при этом оставлены без внимания). Возникает вопрос о том, как автор видит соотношение понятий «технико-криминалистическое средство» и «программное обеспечение и программно-аппаратные комплексы»? Можно ли считать второе частью первого?

2. В положении 7, выносимом на защиту, указаны этапы пошагового алгоритма получения электронной информации, включающие в числе прочих изъятие носителя, полное и частичное копирование, репродукционную съёмку и т. д. Учитывая, что данные действия заявлены как шаги алгоритма, можно предположить, что они являются обязательными для следователя. Однако представляется, что часть этих действий являются альтернативными, а не последовательными. В ходе публичной защиты желательно услышать позицию соискателя по этому вопросу.

3. В положении 8, выносимом на защиту, указано, что при копировании электронной информации, нужно, в числе прочего, создать побитовую копию носителя. В любом ли случае это целесообразно? Сколько, примерно, по мнению автора, займёт изготовление побитовой копии серверного жёсткого диска на 16 ТБ?

4. Поднятый на с. 50–51 вопрос квантовых вычислений, в целом, позиционирован автором правильно, однако цифровые следы (или электронные доказательства) в них не могут формироваться, поскольку квантовые системы не имеют программного обеспечения и пользовательских интерфейсов (интерфейсное окно квантового компьютера представлено в виде

управляющего компьютера по схеме фон Неймана), а квантовое состояние не может сохраняться (кубит разрушается при измерении). Однако сами по себе квантовые вычисления для цифровой криминалистики могут представлять интерес как средство дешифровки сообщений. Интересует мнение автора о конкретных формах использования данной технологии в контексте избранной темы.

5. Представляется, что вопрос опасности систем искусственного интеллекта (параграф 1.3) рассмотрен поверхностно. Кроме того, помимо безусловной опасности этой технологии следовало бы рассмотреть положительные моменты её использования для обнаружения электронных доказательств, то есть как раз «светлую сторону технологии» применительно к выбранной теме, а не в целом для криминалистики.

6. Автор корректно указывает на ограничения получения информации из оперативной памяти (с. 70–73), однако в работе не нашла отражение закономерность современного развития твердотельных накопителей, заключающаяся в усложнении их внутренней структуры и средств защиты информации, что может затруднить в ближайшем будущем корректное получение или восстановление информации с них. Кроме того, в работе содержится противоречие: на с. 70 автор совершенно справедливо относит ОЗУ к электронным носителям информации, в то же время на с. 119 автор указывает, что «оперативная память носителем электронной информации не является».

7. На с. 80 диссертации автор указывает, что файл следует понимать как минимальную единицу электронной информации. При этом в работе не нашёл отражения факт существования файлов-контейнеров, внутри которых также могут содержаться файлы (в том числе другие файлы-контейнеры), примером которых являются любые документы пакета MS-Office, все файлы баз данных, некоторые разновидности файлов расширения .pdf и т. д. Также возникает вопрос, насколько ценным по мнению автора являются метаданные, например, группы EXIF с позиций их доказательственного или идентификационного значения?

8. На с. 119 автор указывает, что «выявление носителей электронной информации происходит визуальным способом». Учитывая, что в работе в ряде случаев фигурировали ситуации получения электронной информации из подключенного к питанию устройства, неясно, почему не рассмотрены программные средства выявления электронных носителей информации, особенно учитывая тот факт, что с их помощью возможно решение поставленных задач по обеспечению достоверности изымаемой информации, в том числе за счёт автоматического расчёта хэш-сумм и выяснения серийных номеров, прошитых на устройстве (что визуальным осмотром, разумеется, не может быть достигнуто).

9. Не совсем понятно, почему автор отказывает аудио- и видеозаписям в статусе электронного документа (с. 77). Современное законодательство (УПК РФ, ГК РФ, ФЗ № 63-ФЗ «Об электронной подписи», ФЗ № 149-ФЗ «Об информации...» и т. п.) предусматривает возможность существования в виде

Сведения:

ФИО: Воронков Дмитрий Валерьевич

Учёная степень: доктор юридических наук по специальности 5.1.4. Уголовно-правовые науки (юридические науки).

Место работы: Уральский государственный юридический университет имени В.Ф. Яковлева

Занимаемая должность: Заведующий кафедрой криминалистики имени И. Ф. Герасимова

Место нахождения учебного заведения: Россия, 620066, г. Екатеринбург, ул.Комсомольская, 21

Телефон: +7 (343) 227-63-63, доб. 1010 Факс: +7 (343) 374-50-34

E-mail: ae@crimlib.info