

УДК 34**Производные методы закрепления электронной информации****Пономарев Виталий Евгеньевич**

Старший преподаватель,
кафедра криминалистики и правовой информатики,
Кубанский государственный университет,
350040, Российская Федерация, Краснодар, ул. Октябрьская, 25;
e-mail: 9529788272@mail.ru

Аннотация

В работе рассматриваются проблемы закрепления электронных доказательств в условиях повсеместной цифровизации, уделяя внимание производным методам фиксации: скриншотам, видеозаписи экрана (скринкастам), репродукционной фотосъемке экрана и прямому захвату видеосигнала. Анализируется практическая потребность в оперативных, простых в исполнении и минимально-инвазивных способах получения доказательственной информации, а также соотношение оперативности и полноты получаемых данных. Отмечено, что производные методы не содержат метаданных исходного носителя и потому требуют строгой процессуальной фиксации — указания источника, времени, форматов, действий исполнителя и условий получения. Представлены рекомендации по применению производных способов, а также краткий перечень необходимого оснащения для их эффективного использования следственными органами.

Для цитирования в научных исследованиях

Пономарев В.Е. Производные методы закрепления электронной информации // Вопросы российского и международного права. 2025. Том 15. № 7А. С. 162-170.

Ключевые слова

Электронные доказательства, закрепление доказательств, скриншот, скринкаст, репродукционная съемка, захват видеосигнала, процессуальная фиксация, метаданные, криминалистическая техника, цифровая криминалистика.

Введение

Проблематика закрепления электронной доказательственной информации в условиях повсеместной цифровизации неизбежно связана с поиском различных методов закрепления, которые обеспечивали бы не только сохранность, но и простату и оперативность применения. При этом, как показывает практика преимущество получают именно наиболее быстрые и наименее технически сложные методы. Именно поэтому большую популярность имеет изъятие электронных носителей информации, вместо их копирования.

Под производными методами понимаются такие методы, при которых доказательственная информация сохраняется не в исходной форме, а в виде производного результата — снимка (скриншота) или видеозаписи экрана (скринкаста), репродукционного фотоснимка или видеозаписи экрана. Производные методы могут применяться в тех случаях, если изъятие носителя электронной информации или прямое копирование технически невозможно или сопряжено с риском утраты данных, либо в тех случаях, когда требуется оперативное закрепление информации, которая легко может быть изменена или уничтожена (например, публикации в сети Интернет).

Особый интерес к производным способам обусловлен тем, что хоть они и предоставляют меньше информации, но они более простые и оперативные, зачастую не требуют особого дополнительного оборудования или технических средств, позволяют закрепить информационную составляющую электронного доказательства практически мгновенно, не требует специальных технических навыков.

Кроме того, такие методы применимы к любому источнику электронной информации, а не только к носителям.

Основное содержание

Согласно орфографическому словарю, скриншот - снимок, картинка, на которой отображено то, что видно на экране компьютера в какой-либо момент [Иванова и др., 2024]. Российское законодательство не содержит понятия снимка экрана или скриншота (от англ. screenshot –снимок экрана). Это не значит, что понятие является новым. Так, Пленум Верховного суда в постановлении №10 от 23 апреля 2019 года в пункте 55 указывает: «допустимыми доказательствами являются в том числе сделанные и заверенные лицами, участвующими в деле, распечатки материалов, размещенных в информационно-телекоммуникационной сети (скриншот), с указанием адреса интернет-страницы, с которой сделана распечатка, а также точного времени ее получения. Такие распечатки подлежат оценке судом при рассмотрении дела наравне с прочими доказательствами (статья 67 ГПК РФ, статья 71 АПК РФ)»[Постановление Пленума ВС РФ № 10, 2019].

Верховный суд таким образом сужает понятие скриншота, определяя несколько признаков, с данной позиции скриншотом признается только распечатка (то есть информация, переведенная в форму бумажного документа), информация материалов, размещенных в сети Интернет, кроме того, такая распечатка должна быть заверена лицом, участвующим в деле. При этом необходимо отметить, что суд указывает на необходимость наличия информации об источнике электронного доказательства: адреса интернет-страницы, времени выполнения.

И.И. Литвин определяет скриншот, как способ захвата изображения с экрана электронного

устройства, результатом которого станет электронный файл в формате изображения [Литвин, 2021, с.90-91].

Исходя из приведенных определений предлагаем выделить признаки скриншота. Во-первых, это изображение экрана, фиксация информации, отображаемой на экране электронного устройства в моменты выполнения записи скриншота. Неверно будет сказать, что это изображение того, что видит пользователь, поскольку, скриншот не отражает и не фиксирует состояние и настройки монитора. Скриншот фиксирует сформированный кадр вывода, вне зависимости от состояния дисплея, даже в случае его отсутствия, неисправности или отключения скриншот все равно будет содержать изображение. Правильнее говорить о том, что скриншот отображает ту информацию, которая передаётся на монитор в конкретный момент времени.

Во-вторых, скриншот выполняется программным обеспечением, установленным на самом устройстве, информация с которого фиксируется. Это может быть как часть операционной системы устройства (например, приложение «Ножницы» в операционных системах семейства Windows), так и специально созданные для этих целей сторонние приложения (например, Lightshot [Skillbrains, [www](http://www.skillbrains.com)]).

В-третьих, результатом выполнения скриншота является создание файла цифрового изображения на устройстве, с использованием которого выполнялся скриншот. То есть визуальной информации, обрабатываемой компьютером или иным устройством, представленная, как правило, в виде массива данных (матрицы) со значениями цвета и яркости каждого отдельного пикселя.

Для скриншота важно, чтобы он был не обрезанный, захватывал изображение экрана целиком, желательно с одновременной фиксацией системного времени.

Видеозапись экрана (скринкастинг) мы считаем самостоятельным производным методом, похожим на создание скриншота по процессу выполнения, но имеющим по сравнению со скриншотами существенные преимущества. Во-первых, видео позволяет показать динамические процессы, например, последовательность действий пользователя или работу программного обеспечения. Во-вторых, видеозапись позволяет фиксировать не только визуальную, но и звуковую информацию. В-третьих, видеозапись значительно более устойчива к подделке, это более трудоёмкая задача, которая требует изменить не статичную картинку, а целую последовательность картинок и последовательность действий.

Причины, по которым видеозапись экрана, как способ фиксации доказательств, используется не часто, на наш взгляд, состоит в том, что её выполнение является более трудоёмкой задачей по сравнению с созданием скриншота. Необходима установка программного обеспечения для создания видеозаписи экрана (Bandicam [Bandicam Company, [www](http://www.bandicam.com)], OBS Studio [OBS Project, [www](http://www.obsproject.com)]). Видеозапись требует большего объема электронного носителя информации для хранения. В использовании, как доказательство видеозапись менее удобна, поскольку её затруднительно, например, распечатать и приложить к протоколу следственного действия.

Некоторые авторы относят к числу скриншотов также изображения, полученные иными способами, например, фото и видеосъёмкой экрана (монитора) компьютера или прямым захватом видеосигнала [Иванова, 2019, с.180-182]. Мы с указанной позицией не согласны, поскольку методы предполагают различный уровень вмешательства в исследуемый объект и позволяют получить различный объем информации. Так, для создания фото или видеосъёмки

монитора компьютера используется внешнее оборудование, а для создания скриншота нужно использовать то оборудование, на котором выполняется снимок экрана. Соответственно в первом случае снимок сохраняется на внешнем устройстве, а во втором на самом оборудовании.

На наш взгляд существует две ситуации в которых следователь может выполнять скриншот для закрепления доказательств. Одна ситуация, когда следователь производит, например, осмотр страницы сайта в сети Интернет и для фиксации информации, размещенной на странице, применяет программное обеспечение, установленное на рабочем компьютере с целью получения скриншота. В дальнейшем полученные следователем скриншоты могут быть перенесены на внешний носитель электронной информации (например CD-диск) и приложены к протоколу осмотра.

Другой случай, когда необходимо зафиксировать информацию, которая отображается на экране смартфона подозреваемого, например, переписку в социальной сети. Соответственно помимо того, что необходимо выполнить скриншоты на устройстве подозреваемого, также, необходимо осуществить перенос полученных скриншотов на иной носитель информации, а процесс такого переноса требует процессуальной фиксации.

Установка, использование на устройстве программного обеспечения, которого там не было изначально, изготовление и скачивание с него скриншотов технически сложный процесс, который сопряжен с вмешательством в исследуемое устройство и может повлечь повреждение или уничтожение доказательственной информации. Гораздо проще и быстрее сфотографировать или записать на видео экран устройства.

Для исключения неоднозначности ситуации с получением информации с чужого устройства такое изъятие на практике может оформляться, как выемка скриншотов, например, согласно материалам уголовного дела были изъяты скриншоты с данными геолокации похищенного мобильного «iPhone 12 Green 256Gb» [Первомайский районный суд г. Краснодара, www]. Мы не считаем изъятые таким способ скриншоты допустимым доказательством, поскольку невозможно установить источники информации, отображенной на скриншоте. Такая информация может быть легко подделана, в том числе с использованием искусственного интеллекта. Изъятые таким образом скриншоты могут быть использованы только в качестве ориентирующей информации.

Еще один метод закрепления доказательственной информации создание репродукционной съемки экрана устройства с использованием внешних технических средств. В этом случае экран устройства снимается при помощи фото или видеокамеры, в тот момент, когда на экране демонстрируется интересующая следователя информация. Сам по себе такой метод не является новым, его рекомендуется применять, например, при обнаружении включенной компьютерной техники [Земцова, Суров, Галушин, 2018].

Репродукционная съемку относят к методам судебно-следственной фотографии [Егоров, 2022, с.79], поскольку её использование возможно без специального лабораторного оборудования. И определяют, как вид фотосъемки, служащий для воспроизведения фотографическим способом плоских оригиналов: чертежей, тестов, схем, рисунков, фотоснимков и т.д. [Афанасьев, Колиев, 2021, с.293]

Считаем, что экран можно считать некоторой разновидностью плоского оригинала и в этом случае съемку экрана с целью фиксации доказательственной информации, отображаемой на экране, можно считать разновидностью репродукционной съемки.

Использование такого способа закрепления имеет существенные преимущества. При

использовании внешних технических средств фиксации вмешательство в источник электронной информации полностью отсутствует, а значит устраняется риск повреждения или утраты доказательственной информации. Второе серьезное достоинство состоит в оперативности такого способа фиксации, поскольку не требуется никаких дополнительных приготовлений, кроме включения внешнего технического устройства для съемки и опционально подготовки штатива.

Из этих преимуществ и того также вытекает отсутствие необходимости наличия у лица, производящего фотографирование каких-либо специальных познаний, кроме необходимых для осуществления фото или видеосъемки. Значит этот способ может применяться следователем в отсутствие специалиста, минимизируя риск повреждения или утраты доказательственной информации.

Одновременно с этим существенный недостаток метода, как упоминалось ранее, состоит в получении изображения худшего качества, чем в случае получения скриншота (снимка экрана). Экран любого устройства состоит из маленьких точек, отображающих цвет – пикселей. И при создании фотографии могут возникать артефакты отображения, артефакты связанные с частотой мерцания экрана. Тем не менее современные фотокамеры и приемы фотосъемки позволяют решить ряд проблем отображения и мерцания экрана, получив изображение приемлемого качества [см. напр.: Nikon Corporation, www].

Указанных недостатков лишен метод прямого захвата видеосигнала - использования аппаратных устройств для перехвата изображения с дисплея в обход штатных функций системы. Для производства захвата видеосигнала используется внешнее оборудование, например, ноутбук и специальное аппаратное устройство, предназначенное для захвата видеосигнала и записи его в файл. В этом случае происходит подключение к источнику электронной доказательственной информации и перехват видеосигнала с него с записью результата в видео или формате изображения на внешнее устройство. При этом вмешательство минимально поскольку перехватывается только идущий на внешнее устройство (монитор) видеосигнал, исключая обратное воздействие на устройство. При этом возможен сквозной захват видеосигнала, то есть одновременная трансляция на экран и запись видео на внешнее устройство.

Для перехвата видеосигнала применяются «карты видеозахвата» - узкоспециализированные аппаратные средства, которые специально созданы для перехвата цифрового или аналогового видеосигнала и записи его в файл [см. напр. AVerMedia, www; Blackmagic Design, www]. Сегодня такие карты создаются и применяются преимущественно в сфере производства медиаконтента для проведения онлайн видеотрансляций, передачи видеосигнала с одного устройства на другое, сохранения или записи видеосигнала с устройства.

Следует отметить, что технически существует возможность шифрования видеосигнала на проводе, в этом случае воспользоваться картой захвата невозможно. Примером такой технологии может выступить HDCP [Digital Content Protection, www]. Однако, такие технологии имеют ограниченную область применения, обычно применяется только для защиты цифрового видеоконтента и сигнал, передаваемый от устройства к экрану, все же как правило, не шифруется.

Считаем, что такие устройства, а точнее аппаратно-программные комплексы на их основе могут найти свое применение в криминалистике для целей закрепления электронных доказательств в некоторых ситуациях. Применение метода захвата видеосигнала может быть

необходимо, когда нет возможности изъять устройство, а доступ к нему для создания скриншотов невозможен, например, ввиду отсутствия на устройстве программного обеспечения, позволяющего создать скриншот или аппаратной возможности скопировать созданные скриншоты на внешний электронный носитель информации. При этом доступен экран, на котором выводится информация, а значит и видеосигнал, доступный для перехвата. В этом случае методы прямой записи видеосигнала могут выступать, как более качественная альтернатива репродукционной съемке экрана устройства.

Метод, в частности, предлагается применять при условии, если копирование файлов по какой-то причине невозможно, для изъятия видеозаписей с систем видеонаблюдения с целью получения наилучшего из возможного качества, что в этом случае очень важно. Об этом говорит стандарт изъятия информации с цифровых систем видеонаблюдения [Video/Imaging Technology & Analysis Subcommittee, 2020]. Зачастую на практике с целью оперативности применяется видеозапись экрана системы видеонаблюдения, причем качество такой видеозаписи зачастую плохое и не позволяет установить детали произошедшего.

Полученное производным способом электронное доказательство не содержит само по себе сопутствующей информации. При создании скриншотов, записей экрана и тем более репродукционной съемке не сохраняются метаданные или любая другая сопутствующая информация, кроме информации, составляющей основу, содержание электронного доказательства. В этой связи доказательства, полученные производным способом, могут быть легко подделаны, особенно с использованием нейросетей систем искусственного интеллекта, созданных на их основе.

В этой связи производные способы могут применяться только следователем самостоятельно, либо следователем при участии специалиста, при этом весь процесс и результат должен быть подробно отражен в протоколе (например, в протоколе осмотра). Необходимо обязательно отражать источник электронной информации – программу, сайт в сети Интернет, файл, а также электронный носитель информации, а также устройство с использованием которого производилась запись скриншота или видеозаписи. Также необходимо указывать на время, формат файла, техническое средство на которое полученные файлы были сохранены. Также в протоколе следует отражать краткое содержание закреплённой таким способом информации. Также указывается лицо, осуществившее действие и подробный перечень действий, выполненных для вывода на экран искомой информации для целей её закреплёния.

Важная мысль в том, что производные методы закреплёния не заменяют первоначальный источник электронного доказательства. Они применяются, только в том случае, если по каким-то иной метод закреплёния неприменим, а электронный носитель информации невозможно изъять.

Производные методы закреплёния электронной доказательственной информации — скриншоты (снимки экрана), запись экрана, репродукционная съёмка экрана и прямой захват видеосигнала — представляют собой оперативные и предусматривающие минимально возможное вмешательство методы, предназначенные прежде всего для закреплёния информации, которая может быть быстро уничтожена или в условиях, когда доступ к носителю электронной информации ограничен или невозможен. Они напрямую зависят от правильной фиксации в протоколе хода и порядка фиксации, источника сведений. При таком подходе производные способы занимают свое место в структуре методов, как эффективное средство, закрывающее потребность оперативно сохранить содержание электронного доказательства.

Заключение

Подводя итог, для эффективного применения производных методов закрепления электронных доказательств в распоряжении у следователя должен иметься персональный компьютер с доступом в информационно-телекоммуникационную сеть Интернет, возможностью делать скриншоты (снимки экрана) и программным обеспечением для производства видеозаписи экрана. Для работы на месте происшествия оборудование для записи экрана устройства – фотоаппарат, в том числе, с возможностью записи видео. Скорее необходимым видится снабжение следователей аппаратно-программными комплексами, позволяющими осуществлять прямой захват видеосигнала. Кроме того, необходимо наличие электронных носителей информации для записи полученной информации с целью последующего использования в качестве доказательств.

Библиография

1. Русский орфографический словарь: около 200 000 слов / О. Е. Иванова, В. В. Лопатин, И. В. Нечаева, Л. К. Чельцова; под ред. В. В. Лопатина, О. Е. Ивановой. — М.: Грамота, 2024. 904 с. (Фундаментальные словари).
2. Постановление Пленума Верховного Суда РФ от 23.04.2019 № 10 "О применении части четвертой Гражданского кодекса Российской Федерации" // "Российская газета", N 96, 06.05.2019.
3. Литвин И. И. К вопросу о соотношении скриншота с фотоснимком в уголовном судопроизводстве / И. И. Литвин // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2021. № 21-1. С. 90-91.
4. Skillbrains. Lightshot — программа для скриншотов [Электронный ресурс]. URL: <https://app.prntscr.com/ru/> (дата обращения: 09.09.2025).
5. Bandicam Company. Bandicam — программа для записи экрана, игр и видеоприложений [Электронный ресурс]. URL: <https://www.bandicam.com/ru/> (дата обращения: 09.09.2025).
6. OBS Project. OBS Studio — бесплатная программа с открытым исходным кодом для записи видео и потокового вещания [Электронный ресурс]. URL: <https://obsproject.com/ru> (дата обращения: 09.09.2025).
7. Иванова Е. В. Скриншот - цифровая возможность в процессе доказывания: проблемные аспекты / Е. В. Иванова // Право и государство: теория и практика. 2019. № 12(180).
8. Приговор Первомайского районного суда г. Краснодара по делу № 1-592/23 УИД 23RS0040-01-2023-005418-80 https://pervomaisky--krd.sudrf.ru/modules.php?delo_id=1540006&name=sud_delo&name_op=doc&new=0&number=319171625&srv_number=1&text_number=1&
9. Земцова С. И., Суров О. А., Галушин П. В. Алгоритм осмотра компьютера при расследовании преступлений, связанных с незаконным оборотом «дизайнерских» наркотиков, совершаемых с использованием интернет-магазинов // Научная сеть «Современное право». 2018. С. 136–142. URL: <https://www.sovremennoepravo.ru> (дата обращения: 09.09.2025).
10. Егоров Н.Н. Криминалистические аспекты производства наглядно-образных способов фиксации доказательств // Пролог: журнал о праве. 2022. №2 (34).
11. Афанасьев Евгений Владимирович, Колиев Вадим Витальевич Современные возможности применения судебной фотографии при производстве осмотра мест происшествия // Право и государство: теория и практика. 2021. №4 (196). С.293.
12. Nikon Corporation. Режим настройки частоты добавлен к функции подавления высокочастотного мерцания // Z 9. Подробное руководство [Электронный ресурс]. URL: https://onlinemanual.nikonimglib.com/z9/ru/updating_high_frequency_flicker_reduction_375.html (дата обращения: 09.09.2025).
13. AVerMedia. Live Gamer Portable 2 Plus (GC513): внешняя карта/рекордер видеозахвата [Электронный ресурс]. URL: <https://www.avermedia.com/product-detail/GC513> (дата обращения: 09.09.2025).
14. Blackmagic Design. DeckLink Mini Recorder 4K: PCIe-карта видеозахвата [Электронный ресурс]. URL: <https://www.blackmagicdesign.com/products/decklink/models> (дата обращения: 09.09.2025).
15. HDCP Specifications // Digital Content Protection. URL: <https://www.digital-cp.com/hdcp-specifications> (дата обращения: 11.09.2025).
16. Standard Practice for Data Retrieval from Digital CCTV Systems: OSAC Proposed Standard. Version 2.0. June 2020 / Prepared by the Video/Imaging Technology & Analysis Subcommittee, Digital/Multimedia Scientific Area Committee

(OSAC for Forensic Science). URL: https://www.nist.gov/system/files/documents/2020/06/26/DMSA_C-VL_Standard%20for%20DVR%20Retrieval_V02_OSA_C%20Proposed_June2020.pdf (дата обращения: 11.09.2025).

Derivative Methods for Fixing Electronic Information

Vitalii E. Ponomarev

Senior Lecturer,
Department of Criminalistics and Legal Informatics,
Kuban State University,
350040, 25 Oktyabrskaya str., Krasnodar, Russian Federation;
e-mail: 9529788272@mail.ru

Abstract

The work examines problems of securing electronic evidence in conditions of widespread digitalization, focusing on derivative fixation methods: screenshots, screen video recording (screencasts), reproductive screen photography, and direct video signal capture. The practical need for operational, easily executable, and minimally invasive methods of obtaining evidentiary information is analyzed, along with the correlation between operational efficiency and data completeness. It is noted that derivative methods lack metadata from the original carrier and therefore require strict procedural fixation - indicating source, time, formats, performer's actions, and acquisition conditions. Recommendations for applying derivative methods are presented, along with a brief list of necessary equipment for their effective use by investigative authorities.

For citation

Ponomarev V.E. (2025). *Proizvodnye metody zakrepleniya elektronnoy informatsii* [Derivative Methods for Fixing Electronic Information]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (7A), pp. 162-170.

Keywords

Justice, obstruction of justice, qualification, investigation, judicial system, preliminary investigation.

References

- 1.Ivanova, O. E., Lopatin, V. V., Nechaeva, I. V., & Cheltsova, L. K. (Eds.). (2024). *Russkii orfograficheskii slovar: okolo 200 000 slov* [Russian spelling dictionary: about 200,000 words]. Gramota. (Fundamentalnye slovari [Fundamental Dictionaries] series).
- 2.Postanovlenie Plenuma Verkhovnogo Suda RF ot 23.04.2019 № 10 "O primeneniі chetvertoi chasti Grazhdanskogo kodeksa Rossiiskoi Federatsii" [Ruling of the Plenum of the Supreme Court of the Russian Federation dated April 23, 2019 No. 10 "On the application of Part Four of the Civil Code of the Russian Federation"]. Rossiiskaia gazeta [Russian Gazette], N 96.
- 3.Litvin, I. I. (2021). K voprosu o sootnoshenii skrinshota s fotosnimkom v ugolovnom sudoproizvodstve [On the correlation between a screenshot and a photograph in criminal proceedings]. *Aktualnye problemy borby s prestupleniiami i inymi pravonarusheniiami* [Actual Problems of Combating Crimes and Other Offenses], (21-1), 90–91.
- 4.Skillbrains. (n.d.). Lightshot — programma dlia skrinshotov [Lightshot — a program for screenshots]. Retrieved September 9, 2025, from <https://app.pmtscr.com/ru/>

5. Bandicam Company. (n.d.). Bandicam — programma dlia zapisi ekrana, igr i videoustroistv [Bandicam — a program for recording the screen, games and video devices]. Retrieved September 9, 2025, from <https://www.bandicam.com/ru/>
6. OBS Project. (n.d.). OBS Studio — besplatnaia programma s otkrytym iskhodnym kodom dlia zapisi video i potokovogo veshchaniia [OBS Studio — free and open-source software for video recording and live streaming]. Retrieved September 9, 2025, from <https://obsproject.com/ru>
7. Ivanova, E. V. (2019). Screenshot - tsifrovaia vozmozhnost v protsesse dokazyvaniia: problemnye aspekty [Screenshot - a digital opportunity in the process of proof: problematic aspects]. *Pravo i gosudarstvo: teoriia i praktika* [Law and State: Theory and Practice], 12(180).
8. Pervomaiskii raionnyi sud g. Krasnodara. (2023). Prigovor po delu № 1-592/23 UID 23RS0040-01-2023-005418-80 [Judgment in case No. 1-592/23 UID 23RS0040-01-2023-005418-80]. Retrieved from https://pervomaisky--krd.sudrf.ru/modules.php?delo_id=1540006&name=sud_delo&name_op=doc&new=0&number=319171625&srv_num=1&text_number=1&
9. Zemtsova, S. I., Surov, O. A., & Galushin, P. V. (2018). Algoritm osmotra kompiutera pri rassledovanii prestuplenii, svyazannykh s nezakonnym oborotom «dizainerskikh» narkotikov, sovershaemykh s ispolzovaniem internet-magazinov [Algorithm for computer inspection during the investigation of crimes related to the illicit trafficking of "designer" drugs committed using online stores]. *Nauchnaia set «Sovremennoe pravo»* [Scientific Network "Modern Law"], 136–142. Retrieved September 9, 2025, from <https://www.sovremennoepravo.ru>
10. Egorov, N. N. (2022). Kriminalisticheskie aspekty proizvodstva nagliadno-obraznykh sposobov fiksatsii dokazatelstv [Forensic aspects of the production of visual-figurative methods of evidence fixation]. *Prolog: zhurnal o prave* [Prologue: Law Journal], 2(34).
11. Afanas'ev, E. V., & Koliev, V. V. (2021). Sovremennye vozmozhnosti primeneniia sudebnoi fotografii pri proizvodstve osmotra mest proisshestviia [Modern possibilities of using forensic photography during crime scene examination]. *Pravo i gosudarstvo: teoriia i praktika* [Law and State: Theory and Practice], 4(196), 293.
12. Nikon Corporation. (n.d.). Rezhim nastroiки chastoty dobavlen k funktsii podavleniia vysokochastotnogo merchaniiia [Frequency setting mode added to the high-frequency flicker reduction function]. *Z 9. Podrobnoe rukovodstvo* [Z 9. Detailed Manual]. Retrieved September 9, 2025, from https://onlinemanual.nikonimglib.com/z9/ru/updates_high_frequency_flicker_reduction_375.html
13. AVerMedia. (n.d.). *Live Gamer Portable 2 Plus (GC513): vneshniaia karta/rekorder videozakhvata* [Live Gamer Portable 2 Plus (GC513): external capture card/recorder]. Retrieved September 9, 2025, from <https://www.avermedia.com/product-detail/GC513>
14. Blackmagic Design. (n.d.). *DeckLink Mini Recorder 4K: PCIe-karta videozakhvata* [DeckLink Mini Recorder 4K: PCIe capture card]. Retrieved September 9, 2025, from <https://www.blackmagicdesign.com/products/decklink/models>
15. Digital Content Protection LLC. (n.d.). HDCP specifications. Retrieved September 11, 2025, from <https://www.digital-cp.com/hdcp-specifications>
16. OSAC Video/Imaging Technology & Analysis Subcommittee. (2020, June). Standard practice for data retrieval from digital CCTV systems: OSAC proposed standard (Version 2.0). National Institute of Standards and Technology. Retrieved September 11, 2025, from https://www.nist.gov/system/files/documents/2020/06/26/DMSAC-VL_Standard%20for%20DVR%20Retrieval_V02_OSA C%20Proposed_June2020.pdf