

Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации
Московский университет Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя

ТЕХНИКО-КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

**Всероссийская научно-практическая конференция,
проводимая в рамках деловой программы
Международной выставки средств обеспечения
безопасности государства «Интерполитех-2024»**

Сборник научных трудов

1 электронный оптический диск (CD-R)
Текстовое электронное издание

Научное электронное издание

Москва
Московский университет
МВД России имени В.Я. Кикотя

2024

© Московский университет МВД России
имени В.Я. Кикотя, 2024
ISBN 978-5-9694-1550-8

УДК 343.98
ББК 67.521
Т38

Рецензенты:

заместитель начальника кафедры противодействия незаконному обороту наркотиков Всероссийского института повышения квалификации сотрудников МВД России **И. В. Канаков**; начальник кафедры криминалистики Белгородского юридического института МВД России имени И.Д. Путилина кандидат юридических наук, доцент **Е. В. Чиненов**

Составитель *И. Н. Горбулинская*

Т38 **Технико-криминалистическое обеспечение раскрытия и расследования преступлений** : Всероссийская научно-практическая конференция, проводимая в рамках деловой программы Международной выставки средств обеспечения безопасности государства «Интерполитех-2024» : сборник научных трудов / [сост. И. Н. Горбулинская]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2024. – 395 с. – 1 электронный опт. диск (CD-R). – Системные требования: CPU 1,5 ГГц; RAM 512 Мб; Windows XP SP3; 1 Гб свободного места на жестком диске.
ISBN 978-5-9694-1550-8

Сборник статей «Технико-криминалистическое обеспечение раскрытия и расследования преступлений» подготовлен коллективом авторов по итогам Всероссийской научно-практической конференции, проводимой в рамках деловой программы Международной выставки «Интерполитех-2024».

Издание адресовано преподавателям, адъюнктам, докторантам, курсантам и слушателям образовательных организаций МВД России.

Научное электронное издание

Минимальные системные требования: CPU 1,5 ГГц; RAM 512 Мб;
Windows XP SP3; 1 Гб свободного места на жестком диске

© Московский университет
МВД России имени В.Я. Кикотя, 2024

Издание подготовлено
с помощью программного обеспечения Microsoft Word

В авторской редакции
Компьютерная верстка *Лосева О. С.*

Подписано к изданию 20.12.2024
Объем издания: 8,6 МБ
1 электронный оптический диск (CD-R)

ISBN 978-5-9694-1550-8



Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12
<https://мосу.мвд.рф>, e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

<i>Абдурагимова Т. И.</i> К вопросу о методах борьбы с мошенническими действиями в сфере интернет-банкинга.....	11
<i>Аладьин А. Н.</i> Технико-криминалистическое обеспечение на объектах железнодорожного транспорта, находящихся под воздействием негативных факторов и окружающей среды	16
<i>Александрова О. В., Енгальчев В. Ф.</i> Технологии виртуальной реальности и искусственный интеллект как инструменты формирования навыков ведения допроса.....	19
<i>Александрова Д. А., Меламед Т. Б., Баберкина Е. П., Якушин Р. В.</i> Исследование хлорсодержащих аварийно химически опасных веществ методом спектрометрии ионной подвижности	23
<i>Аминев Ф. Г.</i> О проблемах внедрения инновационных технологий в технико-криминалистическом обеспечении раскрытия и расследования преступлений	26
<i>Архипова И. А., Пятибратова Н. Д.</i> Оценка результатов проведения судебно-психиатрических экспертиз	30
<i>Белавин А. В., Суворов А. С., Катаев А. С.</i> Некоторые вопросы фиксации огнестрельных повреждений охотничьего оружия в ходе осмотра места происшествия	36
<i>Белодед Д. Р.</i> Формирование психологической устойчивости в информационно-цифровом пространстве как превентивная мера борьбы с преступлениями	41
<i>Беляев М. В., Филимонов А. В.</i> Трасологическое исследование тросовых запорно-пломбировочных устройств на примере изделия «СПРУТ-777М»	45
<i>Букур А. И.</i> К вопросу об использовании инновационных технико-криминалистических средств изъятия объемных следов преступлений, заимствованных из иных отраслей промышленности.....	53
<i>Бобовкин С. М., Диденко Е. А.</i> Проблемы взаимодействия судебных экспертов и субъектов назначения экспертизы на современном этапе.....	56
<i>Владимиров В. Ю., Множина Д. Н.</i> Самодельные зажигательные устройства как объекты криминалистического оружиеведения	61

<i>Газизов В. А., Подволоцкий И. Н.</i> Модернизация методов сравнения в портретной экспертизе с помощью информационных технологий	66
<i>Гольцев Д. С., Несмиянова И. О.</i> К вопросу о необходимости самостоятельного сбора информации судебным экспертом в рамках проведения некоторых видов специальных экспертиз.....	73
<i>Гребнева А. С., Карпов А. Р.</i> Истоки становления кибербезопасности в России	75
<i>Гусев А. Н., Баев М. С.</i> Психологический анализ лицевых экспрессий: перспективы проведения автоматизированных исследований видеозаписей	78
<i>Данилов И. А., Черешнев Р. А.</i> Цифровизация как средство повышения эффективности обеспечения безопасности дорожного движения (передвижные специальные комплексы)...	85
<i>Дядык Е. С.</i> Автоматизация вычисления углов отклонения положения головы фотографируемых лиц при производстве судебной портретной экспертизы	95
<i>Демидова Т. В., Кивель О. В.</i> Типичные экспертные ошибки	100
<i>Демин К. Е.</i> Особенности обнаружения, фиксации и изъятия следов губ человека	104
<i>Дмитриева Л. В.</i> Современные системы видеофиксации и распознавания лиц	109
<i>Донцова Ю. А., Ивашкова А. В.</i> Инновационные средства и методы выявления следов рук при отрицательной температуре	112
<i>Дронова О. Б.</i> Инновационные средства обеспечения технической достоверности вещественных доказательств	118
<i>Жигалов Н. Ю.</i> Криминалистическое обеспечение расследования дистанционного мошенничества	122
<i>Завьялова А. А., Завьялов В. В., Виноградова Н. И.</i> Возможности инструментальной криминалистической идентификации запаховых следов человека	126
<i>Земцова С. И.</i> Грибы, содержащие псилоцибин и (или) псилоцин, как объекты ограниченной оборотоспособности.....	130

<i>Зиганишин М. Н.</i> Технико-криминалистическое обеспечение при расследовании дорожно-транспортных преступлений.....	134
<i>Зуйкова Н. А., Головки С. А.</i> К вопросу о теоретических основах многообъектного исследования подписи ..	139
<i>Каплин А. А.</i> Спектроскопия комбинационного рассеяния бромпроизводных предельных углеводов	141
<i>Караваев И. М., Горбулинская И. Н.</i> Анализ понятийного аппарата, используемого в процессе правового регулирования оборота оружия и боеприпасов	145
<i>Качан В. Н.</i> К вопросу о признаках пуль патронов 7,62×25 мм «ТТ» и 7,63×25 мм «Маузер»	150
<i>Кияева Е. Ю.</i> Использование информационных технологий при составлении фототаблиц на месте происшествия	152
<i>Коглина В. А.</i> Возможности 3D-микроскопии при установлении относительной давности изготовления реквизитов документов.....	159
<i>Коновалова М. А.</i> Киберпреступления: возможности использования специальных знаний и вопросы предупреждения	164
<i>Корниленко А. В.</i> Идентификация автора материалов, размещенных в сети Интернет и содержащих признаки запрещенной информации: оперативно-разыскная практика	168
<i>Коровкин Д. С.</i> Дульнозарядные стреляющие устройства, встречающиеся в судебной экспертной практике, и их конструктивные особенности	172
<i>Крюкова Е. С.</i> Искусственный интеллект в криминалистической деятельности: за и против ...	182
<i>Кузовлев В. Ю.</i> Синтетические психоактивные вещества в системе классификации оружия массового поражения: экспертологический подход к распознаванию новых угроз Российской Федерации	186
<i>Лавелина В. В., Пономарев В. В.</i> Архивные документы как объекты дактилоскопической экспертизы	192

<i>Лантух Э. В., Лантух Н. В.</i> Технико-криминалистическое обеспечение раскрытия и расследования преступлений в России и за рубежом: взгляд в будущее.....	198
<i>Мокробородов Л. С., Ковалева Л. С.</i> Спектрометрия ионной подвижности фенола.....	202
<i>Маслов Н. В.</i> Особенности тактики допроса при расследовании групповых преступлений....	205
<i>Нестеров А. В.</i> О некоторых проблемах применения специальных знаний при расследовании преступлений в виртуально-информационном пространстве	209
<i>Никитина И. Э.</i> Инновационные решения в сфере технико-криминалистического обеспечения предупреждения преступлений....	214
<i>Новиков Ф. А.</i> Использование возможностей эмоционального интеллекта в экспертном исследовании преступлений, совершаемых с использованием цифровых технологий	219
<i>Пакалина Д. И.</i> Участие специалиста в области технико-криминалистического исследования документов в оперативно-разыскной деятельности	223
<i>Бондаренко Р. В., Рыбалкин Н. А.</i> Генезис исследования документов при производстве судебной экспертизы.....	227
<i>Поташов М. Р.</i> Предложения по ограничению возможности инвестирования в акции производителей каннабиса на территории Российской Федерации	231
<i>Пучков Г. Ю.</i> О возможностях использования фенотипических признаков человека в правоохранительной деятельности.....	238
<i>Решняк О. А.</i> Возможности использования искусственного интеллекта в криминалистике....	242
<i>Ромашенко О. Л., Карранса Л. К.</i> К вопросу о совершении преступлений в сфере оборота криптовалюты биткойн в Республике Эль-Сальвадор	244
<i>Рослова О. Е.</i> Изучение динамического стереотипа как элемента когнитивных особенностей исполнителя при исследовании потенциально поддельных подписей	248

<i>Сафонов А. А., Суляева А. С.</i> Еще раз к вопросу о возможности внедрения технологий искусственного интеллекта в криминалистическую деятельность	252
<i>Сезонова Т. В.</i> К вопросу об использовании видео-конференц-связи при проведении некоторых следственных действий.....	255
<i>Синюк В. Д.</i> Развитие специальной техники экспертно-криминалистического сопровождения расследования взрывов и пожаров в МВД России.....	258
<i>Соколова О. А.</i> Принципы использования технологии искусственного интеллекта в судебно-экспертной деятельности.....	261
<i>Степанова Д. В., Лузенина Л. А.</i> Спектрометрия ионной подвижности насыщенных гетероциклических соединений	264
<i>Сумина А. В., Лукинский И. С.</i> Технико-криминалистическое обеспечение: теоретический и практический аспекты	269
<i>Тарасов Д. А.</i> Возможности использования нейросетей в экспертных исследованиях.....	275
<i>Теткин Д. В.</i> Возможности применения искусственного интеллекта (нейросети) в деятельности следователя в процессе работы с процессуальными и иными документами	278
<i>Токарева Е. В.</i> Единообразие и стандартизация форм экспертных выводов как основа объективной оценки экспертных заключений	285
<i>Трушакова Н. А.</i> Совершенствование способов изготовления и фальсификации документов: корреляционная связь.....	288
<i>Трущенко И. В., Тимофеев И. И.</i> Использование комплекса «Виртуальный криминалист» в преподавании юридических дисциплин	291
<i>Тумакова П. Б.</i> Прогнозы совершенствования биометрических систем распознавания лиц ...	294
<i>Тюрина А. Ю., Рябухина М. В., Одинокоев Г. Н.</i> Применение методов ДНК-анализа при исследовании объектов животного и растительного происхождения	298

<i>Фаниев П. А.</i> К вопросу необходимости предварительного исследования цифровых следов при проведении процессуальных действий и оперативно-разыскных мероприятий.....	302
<i>Федорович В. Ю.</i> К вопросу о профилактике подделки оттисков печатей с воспроизведением Государственного герба Российской Федерации	305
<i>Фомина Е. С., Батыров Т. С.</i> Использование технологий поиска, сбора, обработки и анализа данных из открытых источников в практике применения полиграфа	309
<i>Хомяков Э. Г.</i> Технологии работы с цифровыми следами в криминалистике	312
<i>Хрусталева В. Н.</i> Место и значение технико-криминалистического обеспечения в системе научно-технического обеспечения судопроизводства.....	317
<i>Цветкова О. К.</i> Роль заключения эксперта в расследовании уголовных дел в области безопасности дорожного движения и эксплуатации транспортных средств. Тактика назначения экспертиз.....	327
<i>Чубарь И. А., Кудряшов Д. А., Злобин С. Г.</i> Пули и гильзы со следами оружия как объекты машинного обучения автоматизированных баллистических идентификационных систем.....	333
<i>Чулахов В. Н.</i> Причины малой эффективности выявления криминалистической информации из вещной обстановки преступления	337
<i>Шавленко В. Н.</i> Применение современных средств стабилизации изображения при фотосъемке в ходе проведения следственных действий	341
<i>Шуваева М. С.</i> Правовые основы и особенности организации технико-криминалистического обеспечения расследования преступлений.....	347

Трибуна Молодого Ученого

<i>Ашихмина В. С.</i> Использование специальных знаний при расследовании преступлений, совершаемых с использованием информационных технологий: актуальные проблемы и перспективы развития.....	352
<i>Ерышева А. Д.</i> Использование 3D-технологий при осмотре места происшествия	356

<i>Жукова А. Р.</i> Применение аддитивных технологий для создания огнестрельного оружия: современное состояние и возможные последствия	359
<i>Кулешова И. А.</i> Личность преступника как основной элемент криминалистической характеристики преступлений против половой неприкосновенности и половой свободы (на основе статистических данных)	363
<i>Ле Суан Хоанг</i> Конструктивные особенности письменных знаков современного вьетнамского алфавита, влияющие на производство судебно-почерковедческой экспертизы малообъемных рукописей, выполненных вьетнамской письменностью	367
<i>Мазова В. Д.</i> Видеофиксация и звукозапись при производстве допроса в уголовном процессе	372
<i>Мищенко В. И.</i> Сравнительный анализ организации исследования наркотических средств в России и Италии	376
<i>Новикова А. А.</i> Возможности исследования особенностей почерка амбидекстров для решения экспертных задач	378
<i>Салапин М. А.</i> Современные особенности использования беспилотных воздушных судов органами полиции в ходе фиксации доказательственной информации	382
<i>Семенова У. С.</i> Возможности искусственного интеллекта. Его применение в криминалистике	386
<i>Фан Куок Тхань</i> К вопросу о собирании электронных данных при расследовании киберпреступлений в Социалистической Республике Вьетнам	389
<i>Яковлева Д. В.</i> История и причины запрета безрецептурной продажи кодеина	393

Хомяков Э. Г.¹,

доцент кафедры

уголовного процесса и криминалистики

Института права, социального управления и безопасности

Удмуртского государственного университета,

кандидат юридических наук, доцент

ТЕХНОЛОГИИ РАБОТЫ С ЦИФРОВЫМИ СЛЕДАМИ В КРИМИНАЛИСТИКЕ

10 октября 2024 г. на координационном совещании в Генеральной прокуратуре Российской Федерации рассматривались вопросы противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, цифровой валюты и компьютерной информации [1]. В ходе данного совещания Генеральный прокурор Российской Федерации И. В. Краснов, отмечая низкую раскрываемость данных преступлений и недостаточную эффективность их расследования, указал на то, что «повышение раскрываемости ИКТ-преступлений во многом зависит от эффективности деятельности оперативных и следственных подразделений, оснащения их необходимым программным обеспечением, оборудованием и квалифицированными специалистами».

В большинстве современных научных исследований, посвященных цифровизации уголовного судопроизводства, говорится о необходимости соответствующей подготовки сотрудников правоохранительных органов, направленной на формирование компетенций, необходимых для работы с разнообразными цифровыми устройствами (ноутбуками, айфонами, смартфонами, серверами, цифровыми камерами, системами «умного дома», бортовыми компьютерами транспортных средств и т. д.), несущими информацию о событии преступления. Подобная криминалистически значимая компьютерная информация, т. е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, характеризуется как цифровые следы [2, с. 7; 3, с. 97]. В настоящее время именно термин «цифровые следы» является одним из наиболее распространенных в научной и учебной литературе по цифровой криминалистике; появилось учение о цифровых следах [4, с. 40–57]. При этом дискуссии о сущности данных следов активно ведутся.

Представление цифровых следов через криминалистически значимую компьютерную информацию, наверное, в большей степени подходит для уголовного процесса, чем для криминалистики.

Возможно в криминалистике лучше рассматривать цифровые следы как совокупность данных, остающихся в результате любой активности субъекта в цифровом пространстве в связи с событием преступления. В этой связи целесообразно напомнить о том, что одной из разновидностей судебной компьютерной (компьютерно-технической) экспертизы является экспертиза информации (данных), на разрешение которой ставятся вопросы, связанные именно

¹ © Хомяков Э. Г., 2024.

с данными, находящимися на представленных на экспертизу носителях информации [5, с. 70–71; 6].

Природу цифровых следов следует рассматривать в двух аспектах.

Материальный аспект цифровых следов проявляется в том, что для их существования требуется физическая среда – цифровые (электронные) носители данных, процессоры, сети передачи данных и т. д.

Идеальный аспект цифровых следов проявляется в том, что, как и другие формы информации они воспринимаются людьми как абстрактные сущности, которые можно передавать через различные носители без изменения их содержания.

Среди цифровых следов, представляющих интерес для следствия, можно выделить файловые следы (удаленные, скрытые, измененные, временные (кеш) файлы, cookie-файлы); сетевые следы (логи подключений, сетевой трафик, IP-адреса, DNS-запросы); следы операционной системы (системные журналы; данные о запуске программ; системные ошибки); метаданные (временные метки, геолокация).

Вследствие сложной природы цифровых следов для работы с ними требуются соответствующие знания, умения и навыки, а также технико-криминалистические средства, приемы и методы.

В общем виде работа с цифровыми следами в ходе отдельных следственных действий, например, осмотра места происшествия, обыска и выемки, может быть сведена к следующему.

1. Поиск цифрового устройства – носителя цифровых следов.

2. Фиксация цифрового устройства – его описание в протоколе следственного действия, фото- или видеосъемка. При описании указываются все подключения (сопряжения) цифрового устройства через соответствующие разъемы (порты) с указанием подключенных объектов.

3. Если цифровое устройство выключено, то производится его отстыковка от всех подключений (путем отсоединения кабелей), упаковка и изъятие; при возможности для упаковки целесообразно использовать чехлы (сумки) Фарадея (англ. Faraday Bag), экранирующие (блокирующие) все радиосигналы и беспроводные каналы связи.

После изъятия цифрового устройства поиск и исследование цифровых следов на нем должны производиться экспертом в рамках судебной компьютерной (компьютерно-технической) экспертизы.

4. При обнаружении включенного цифрового устройства в описании должны быть отражены активные сетевые подключения. При их наличии необходимо немедленное отключение цифрового устройства от сети (либо через отключение кабеля Ethernet, либо отключение Wi-Fi через физическую кнопку на устройстве (если такая есть), либо с помощью сетевых настроек; альтернативный вариант – поместить цифровое устройство в чехол Фарадея, что полностью заблокирует доступ к беспроводной сети).

Также необходимо произвести фотосъемку экрана цифрового устройства (при его наличии), фиксирующую все открытые программы, активные окна,

текстовые сообщения и другую информацию (с соответствующим описанием в протоколе следственного действия).

Не следует пытаться самостоятельно (без специалиста) закрывать программы, перемещать файлы или пытаться разобраться в содержимом цифрового устройства. Важно помнить, что даже перемещение курсора или взаимодействие с операционной системой может изменить журналы событий, временные метки файлов или активировать автосохранение файлов.

5. С помощью аппаратных и программных средств произвести копирование данных из оперативной памяти (ОЗУ) и с иных носителей информации цифрового устройства. Для этого в качестве аппаратных средств могут использоваться блокировщики (копировщики) данных (англ. write blocker) – устройства, предотвращающие изменение данных при копировании с оригинального носителя либо магнитные, оптические, твердотельные накопители; в качестве программных средств – специализированные программы для криминалистического анализа данных, например, EnCase, FTK, Autopsy, Wireshark, Belkasoft Live RAM Capturer и другие либо их отечественные аналоги.

После проведенных операций цифровое устройство выключается, его отсоединяют от всех подключений, упаковывают и изымают; при возможности для упаковки также используют чехлы (сумки) Фарадея.

Все действия с включенными и выключенными цифровыми устройствами следователь должен выполнять совместно со специалистом, в качестве которого целесообразно привлекать судебного эксперта, имеющего право самостоятельного производства судебной компьютерной (компьютерно-технической) экспертизы и обеспеченного соответствующими технико-криминалистическими средствами.

Следователи, как правило, не обладают квалификацией экспертов в области цифровой криминалистики. Это приводит к необходимости разработки методик и стандартов, которые позволяют минимизировать риск утраты или искажения данных на этапе первичного осмотра. Ключевая задача следователя при производстве любых следственных действий, связанных с обнаружением цифровых устройств – обеспечить их сохранность и изоляцию от внешних воздействий до передачи эксперту.

Следует помнить, что различные операционные системы требуют разных подходов к копированию информации с цифровых устройств. А после копирования информации необходимо принятие мер по ее сохранению в процессе хранения как самих цифровых устройств, так и накопителей с откопированной информацией.

Кроме этого, следует помнить о том, что при копировании файлов с одного носителя на другой некоторые параметры файлов могут изменяться, например, могут измениться временные метки, атрибуты файла, его местоположение и физическое положение на новом носителе информации.

В случае с физически поврежденными носителями или системными сбоями при копировании могут возникнуть ошибки, которые приведут к частичной или полной потере данных.

Необходимо также отметить, что одним из ключевых инструментов для фиксации цифровых следов и защиты данных от изменений является хэширование – процесс преобразования данных (файла, текстового сообщения и т. д.) в строку фиксированной длины с помощью математической функции (хэш-функции). Хэширование используется для проверки целостности и достоверности данных, а также их дальнейшей идентификации. Когда файл или набор данных проходит через хэш-функцию, на выходе получается уникальная строка (хэш, хэш-сумма, хэш-код), которая однозначно соответствует содержимому файла.

Хэшированию могут подвергаться как отдельные файлы, так и весь набор файлов на цифровом (электронном) носителе информации. Хэширование всего содержимого носителя (образа диска) обычно используется для криминалистического анализа. Вместо создания отдельных хэшей для каждого файла генерируется один хэш для образа диска – точной копии всего содержимого носителя; такой метод позволяет сохранить всю файловую структуру и метаданные носителя.

Хэширование обычно выполняется до и после копирования файлов путем использования специальной компьютерной программы (утилиты); подобная функция хэширования имеется, например, в EnCase или FTK Imager. Хэш-код (англ. Hash code) – это хэш-значение, сгенерированное для конкретных данных (файла, группы файлов или всего носителя), которое используется как уникальный идентификатор этих данных (до и после копирования). Она позволяет подтвердить, что информация не была изменена или повреждена.

Таким образом, хэш-код может считаться характеристикой цифрового следа, так как он описывает его уникальное состояние на момент фиксации.

Хэш-код (хэш-сумма) идентифицирует цифровой след; он подтверждает целостность и достоверность данных (если сравнивается с исходным значением) и является неотъемлемой частью описания цифрового следа в криминалистическом контексте.

Цифровые следы в данном случае можно рассматривать как совокупность данных, остающихся в результате любой активности субъекта в цифровом пространстве в связи с событием преступления и закрепленных в процессе фиксации хэш-кодом.

Подобный порядок (алгоритм, регламент) по работе с цифровыми устройствами, подкрепленный необходимым инструментарием и направленный на фиксацию цифровых следов, связанных с ними, может рассматриваться как одна из технологий, которая должна быть в арсенале современного следователя и специалиста. Безусловно в зависимости от вида цифровых следов, цифровых устройств и цифровых (электронных) носителей информации, а также поставленных задач соответствующий порядок работы, а также необходимый инструментарий могут меняться, что должно найти отражение в нормативных документах или стандартах, которые могли бы стать основой цифровизации криминалистической деятельности на современном этапе.

Список литературы

1. Официальный сайт Генеральной прокуратуры Российской Федерации. Мероприятия и встречи. URL: <https://epp.genproc.gov.ru/web/gprf/mass-media/events-and-meetings?item=98418092>.
2. Цифровые следы преступлений / [А. М. Багмет и др.]. М. : Проспект, 2021.
3. Цифровая криминалистика : учебник для вузов / [В. Б. Вехов и др.] ; под ред. В. Б. Вехова, С. В. Зуева. 2-е изд., перераб. и доп. М. : Юрайт, 2024.
4. Теория информационно-компьютерного обеспечения криминалистической деятельности: монография / под ред. Е. Р. Россинской. М. : Проспект, 2022.
5. Методы и способы получения доказательственной информации с электронных носителей : учебное пособие / сост. М. В. Старичков, А. А. Шаевич. Иркутск : ВСИ МВД России, 2015.
6. Сайт Федерации судебных экспертов. Компьютерная экспертиза. URL: <https://sud-expertiza.ru/kompyuternaya-ekspertiza/>.