

ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

**ТАКТИКА ОБНАРУЖЕНИЯ, ФИКСАЦИИ И ИЗЪЯТИЯ СЛЕДОВ,
ХРАНЯЩИХСЯ В КИБЕРПРОСТРАНСТВЕ**
Методические рекомендации

Воронеж 2026

Рассмотрено и одобрено на заседании кафедры криминалистики, протокол № 6 от 11 февраля 2026 г.

Рассмотрено и одобрено на заседании методического совета, протокол № 6 от 16 февраля 2026 г.

Рассмотрено и рекомендовано к изданию на заседании редакционно-издательского совета, протокол № 2 от 24 февраля 2026 г.

Рецензенты:

О.К. Исаева – заместитель начальника отдела экспертно-криминалистических учетов ЭКЦ ГУ МВД России по Воронежской области кандидат юридических наук;

Н.А. Лещева – заместитель начальника КМО ГСУ ГУ МВД России по Воронежской области.

Тактика обнаружения, фиксации и изъятия следов, хранящихся в киберпространстве : методические рекомендации / Е.А. Пидусов, Е.И. Пырьева, О.О. Сахно – Воронеж: Воронежский институт МВД России, 2026. –36 с.

В методических рекомендациях рассмотрено понятие киберпространства, проанализированы электронно-цифровые следы как типичные следы киберпреступлений; выявлена специфика механизма образования следов в киберпространстве; проведен анализ тактики следственных действий как средства фиксации доказательственной информации, хранящейся в киберпространстве. Методические рекомендации могут быть использованы в методическом обеспечении деятельности следователей, в образовательном процессе Воронежского института МВД России при изучении дисциплин «Методика расследования отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий», «Расследование отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий».

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	4
1. Понятие киберпространства и специфика механизма образования электронно-цифровых следов как типичных следов киберпреступлений.....	8
2. Деятельность следователя по поиску(обнаружению) и фиксации следов в кибернетическом пространстве.....	16
3. Тактика производства отдельных следственных действий как средство фиксации доказательственной информации, хранящейся в кибернетическом пространстве.....	24
ЗАКЛЮЧЕНИЕ.....	32
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	34

ВВЕДЕНИЕ

В современном мире наблюдается активное развитие информационных технологий, широко внедряются цифровые средства видеозаписи, звукозаписи, фотосъемки, а также мобильные телефоны, которые стали неотъемлемой частью повседневной жизни каждого человека и общества в целом. Данные технологии находятся в постоянном и интенсивном процессе своего развития, что вызвало появление новой сферы коммуникаций (включая в сети «Интернет»), именуемой как «кибернетическое пространство», которое определяется как среда, в которой отражаются преступления, связанные с информационными технологиями, и появляется новый вид следов — электронно-цифровых.

Укрепление и рост роли киберпространства как интерактивной информационно-телекоммуникационной среды привело к возникновению угроз, связанных с уязвимостью информационной инфраструктуры. Развитие и совершенствование информационно-телекоммуникационных технологий стимулирует интерес к ним со стороны преступников, которые используют их в качестве инструментов реализации новых криминальных схем совершения преступлений и сокрытия их следов. Вследствие этого рассмотрение вопроса поиска электронно-цифровых следов киберпреступлений, механизма следообразования позволит расширить возможности органов предварительного расследования в этой области и повысить эффективность расследования данных деяний.

За январь-июль 2025 года зарегистрировано 424,9 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Это на 2,3% меньше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 38,9% в январе-июле 2024 года до 39,2%. Больше половины преступлений в

киберпространстве (51,8%) относится к категориям тяжких и особо тяжких (220,1 тыс.) По сравнению с прошлым годом их число выросло на 7,4%. Почти две трети таких преступлений (62,5%, или 265,6 тыс.) совершается путем кражи или мошенничества, почти каждое шестое (17,2%, или 73,0 тыс.) - с целью незаконного производства, сбыта или пересылки наркотических средств (рост на 51,6%).

Ущерб от IT-преступлений в России за семь месяцев текущего года увеличился на 16% - с 100,5 млрд рублей до 119,6 млрд рублей¹.

Для преступлений в киберпространстве характерен особый механизм их совершения, различающийся в зависимости от конкретных видов преступлений, что обусловлено уникальной информационной средой, в которой реализуются преступные намерения злоумышленников.

В киберпространстве, как уникальной информационной среде отражаются, фиксируются и сохраняются электронно-цифровые следы, оставляемые в результате самой разной человеческой деятельности, в том числе носящей криминальный характер.

Процедура поиска электронно-цифровых следов преступлений, совершаемых в кибернетическом пространстве, является творческой задачей, требующей глубоких и всесторонних знаний, нестандартного мышления и широкого кругозора. Способы и методы сокрытия данных следов совершенствуются одновременно с развитием информационно-телекоммуникационных технологий.

Подобное положение обострило необходимость постановки вопроса о разработке тактических рекомендаций по обнаружению, фиксации, изъятию электронно-цифровых следов, и тактике отдельных следственных действий по преступлениям, совершенным в киберпространстве.

¹ Состояние преступности за 2020 – 2025 годы. [Электронный ресурс] – URL: <https://мвд.рф/reports/item/60248328/> (дата обращения: 15.09.2025).

Объектом исследования выступают общественные отношения, возникающие в связи обнаружением, фиксацией и изъятием следов, хранящимся в киберпространстве.

Целью работы является рассмотрение вопросов обнаружения, фиксации и изъятия следов, хранящимся в киберпространстве.

Для достижения указанной цели проведен анализ научной литературы, статистических данных, определено понятие киберпространства, проанализированы электронно-цифровые следы киберпреступлений и механизм их образования; проведен анализ тактики отдельных следственных действий как средства фиксации доказательственной информации, хранящейся в киберпространстве.

Практическое значение данной работы обусловлено, во-первых, необходимостью методического обеспечения учебного процесса образовательных организаций МВД России при преподавании следующих учебных дисциплин: «Методика расследования отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий», «Расследование отдельных видов преступлений, совершенных с использованием информационно - телекоммуникационных технологий»; во-вторых, необходимостью методического обеспечения деятельности следователей при расследовании преступлений, совершённых в киберпространстве.

1. Понятие киберпространства и специфика механизма образования электронно-цифровых следов как типичных следов киберпреступлений

Прежде чем перейти к анализу электронно-цифровых следов киберпреступлений и специфике механизма их образования в киберпространстве, следует рассмотреть различные подходы к определению понятия «киберпространство», дать им обоснованную оценку, в том числе с позиции криминалистики, поскольку практически каждое преступное действие с использованием ИТ-технологий оставляет электронно-цифровые следы в киберпространстве.

Прежде всего, стоит обратить внимание на отсутствие единого подхода к наименованию определяемого явления. Встречаются такие формулировки, как виртуальное пространство, информационная среда, киберпространство. Так, Е.С. Переверзева употребляет термин «виртуальное пространство», указывая, что это «среда, в которой возникают, изменяются и прекращаются информационные отношения на основе комплекса средств, позволяющих обеспечить непрерывное протекание информационных процессов»¹.

Е. Н. Яковец, применяет категорию «информационное пространство» (информационная сфера)². В законодательстве данный термин используется в Указе Президента РФ от 9 мая 2017 г. № 203³. По нашему мнению, данная формулировка не раскрывает компьютерную, кибернетическую сущность

¹Переверзева Е. С. Виртуальные и цифровые следы: новый подход в понимании / Е. С. Переверзева, А. В. Комов // Вестник Санкт-Петербургского университета МВД России. – 2021. – № 1(89). – С. 176.

²Яковец Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации : учебное пособие / Е. Н. Яковец. – Москва, 2017. – С. 204.

³Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента РФ от 9 мая 2017 г. № 203 // Собрание законодательства РФ. – 2017. – № 20. – Ст. 2901.

пространства.

В Модельном законе «О противодействии киберпреступности» киберпространство (кибернетическое пространство) определяется как цифровая среда (цифровое пространство), возникающая в результате взаимодействия людей, программного обеспечения и сервисов в информационно-телекоммуникационных сетях, включая сеть «Интернет», посредством связанных с ними технологических устройств и сетей, существующую в физической форме.¹ На наш взгляд именно термин «киберпространство» является наиболее точным, поскольку он отражает сущность данного понятия.

Далее следует рассмотреть существующие в юридической науке точки зрения относительно определения понятия «киберпространство».

Д. Д. Штодина полагает, что киберпространство — это уникальный режим физических и виртуальных объектов, средств аппаратного обеспечения (hardware) и программного обслуживания (software), то есть всех компьютерных сетей, существующих в мире, в том числе сеть «Интернет» и другие сети, обособленные или не подключенные к сети «Интернет». Следовательно, киберпространство включает сеть «Интернет», является более широким в сравнении с ним понятием и потому не сводится лишь к нему².

С криминалистических позиций рассматривает понятие «киберпространство» В. А. Мещеряков, понимая его как на динамическую среду присутствия человека, образуемую следующими элементами:

¹ Модельный закон о противодействии киберпреступности (Принят 14.04.2023 в г. Санкт-Петербурге Постановлением 55-20 на 55-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ) // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. – 2023. – № 78 (часть 3).

²Штодина Д. Д. Международно-правовой режим киберпространства: позиция США : дис. ... канд. юрид. наук / Д. Д. Штодина. – Москва, 2023. – С. 29–30.

- 1) информационно-технической инфраструктурой компьютерных систем и их сетей;
- 2) системой информационно-цифровых объектов, созданных и функционирующих в этой инфраструктуре;
- 3) системой акторов (пользователей, а также созданных ими компьютерных программ), использующих для решения целевых задач информационно-цифровые объекты в инфраструктуре компьютерных сетей;
- 4) установленными правилами (протоколами) сетевого взаимодействия всех выше указанных элементов¹.

На основании проведенного анализа различных подходов к пониманию киберпространства, можно прийти к заключению о том, что во всех предлагаемых вариантах имеется одна общая черта. Речь идет о признании киберпространства в качестве некоторой абстрактной виртуальной реальности, существующей исключительно в рамках средств компьютерной техники.

Далее закономерно возникает вопрос, чем же тогда отличается киберпространство от информационной сети, например, сети «Интернет».

По этому вопросу М. А. Простосердов отмечает, что появление киберпространства возможно в любой информационно-телекоммуникационной сети, включая сеть «Интернет». В рамках последней говорят об «Интернет-пространстве». На основании этого автор утверждает, что «Интернет» – это только условие, в котором киберпространство может существовать².

По нашему мнению, сеть «Интернет» – это своего рода реальное материальное отражение киберпространства. Данная сеть представлена

¹Мещеряков В. А. Теоретические основы механизма слепообразования в цифровой криминалистике : монография / В. А. Мещеряков. – Москва, 2022. – С. 33.

²Простосердов М. А. Указ. соч. – С. 22.

отдельными компьютерами, серверами и другими техническими устройствами, соединенными между собой проводным и беспроводным путем по всему миру (через микроволновые и электромагнитные сигналы, спутник, Wi-Fi и т.д.). Это и есть всемирная (глобальная) информационно-телекоммуникационная сеть.

Таким образом, сеть «Интернет» есть часть киберпространства, поскольку последнее включает в себя сеть «Интернет», социальные сети, веб-сайты, электронную почту, электронную коммерцию, онлайн-игры и прочие аналогичные платформы (сервисы). Сама сеть «Интернет», будучи глобальной, образуется тремя слоями: «большой» интернет; глубокий (невидимый) интернет; темный интернет.

Под киберпространством понимается область взаимодействия средств компьютерной техники, компьютерных систем (сетей), компьютерных программ пользователей, а также данные, циркулирующих в этих элементах.

Посягательства, которые совершаются в «киберпространстве», именуются киберпреступлениями, под которыми понимается преступное посягательство, посягающее на разнородные общественные отношения, совершаемое с использованием средств компьютерной техники, информационно-телекоммуникационных сетей и организованного ими киберпространства.

При расследовании преступлений, совершенных в киберпространстве следователь сталкивается с необходимостью работы с электронно-цифровыми следами. Восприятие таких следов для следователя затруднено и требует наличия у него определенных навыков.

Считаем важным рассмотреть само понятие «электронно-цифровой след», поскольку такие следы являются типичными для киберпреступлений, и образуются они в результате каждого выхода в киберпространство (включая сеть Интернет) с помощью компьютера, планшета, мобильного

средства сотовой связи и любых других цифровых устройств.

По мнению А.Ю. Самойлова, электронно-цифровыми являются следы, образующиеся на носителях информации или передающиеся по проводным каналам связи (радиоканалам) в виде электромагнитных сигналов¹.

В представлении Е.В. Смахтина, «электронно-цифровой след» — это любая криминалистически значимая компьютерная информация, зафиксированная на материальном носителе путем электромагнитных взаимодействий или транслируемая по каналам связи посредством электромагнитных сигналов².

Электронно-цифровыми следами, по сути, является компьютерная информация, содержащаяся в файлах, на электронных носителях. Это, в частности, дампы оперативной памяти; дампы трафиков; файлы, созданные программными и аппаратным средствами; цифровая информация, содержащаяся на материальных носителях³.

Все преступления, совершаемые в киберпространстве, образуют различные электронно-цифровые следы. Так, кибермошенничество с использованием сети Интернет приводит к образованию многочисленных электронно-цифровых следов. Например, это такие следы, как: регистрационные данные доменного имени; log-файлы и иные следы, появившиеся в результате взаимодействия с регистратором доменных имен; следы при настройке DNS-сервера, поддерживающего домен кибермошенников; данные аккаунта пользователя; переписка с жертвами; следы ввода и вывода денежных средств; следы управления счетами.

¹ Самойлов А.Ю. Особенности фиксации цифровых следов в ходе проведения следственного осмотра // Сетевое издание «Академическая мысль». – 2020. – № 2 (11). – С. 97.

² Смахтин Е.В. Цифровые технологии и криминалистика: некоторые проблемные аспекты // Российский юридический журнал. – 2018. – № 4. – С. 79.

³ Семикаленова А.И. Цифровые следы: назначение и производство экспертиз // Вестник Университета имени О.Е. Кутафина. – 2019. – № 5. – С. 116.

При незаконном распространении вирусных компьютерных программ образуются такие электронно-цифровые следы, как: коды данных программ, программные средства управления ими, отчеты и статистика антивирусного ПО. Данные следы могут находиться на серверах и интернет-сайтах, компьютерных устройствах жертвы и киберпреступника.

При удаленном неправомерном доступе к компьютерной информации в памяти компьютерных устройств остаются в большинстве случаев следующие виды электронно-цифровых следов: посещенные веб-сайты, отправленные электронные сообщения, информация, указанная в онлайн-формах.

По нашему глубокому убеждению, сущность электронно-цифровых следов состоит в отображении изменений информации, содержащейся на электронных носителях, относительно ее исходного состояния.

Механизм следообразования в киберпространстве представляет собой особую форму протекания процесса, в результате которой образуется след, обусловленный спецификой следового контакта. Следовоспринимающим объектом здесь будет информация, которая передается в первую очередь при помощи электронно-цифровых носителей данных сохраняется во времени и подвергнута обработке.

Следует отметить, что механизм следообразования в кибернетическом пространстве отличается от механизма взаимодействия объектов материального мира. Эта особенность состоит в отсутствии у электронно-цифрового следа пространственной формы, внутреннего строения, а также в способах преобразования и недоступности непосредственного восприятия. В основе этого механизма лежит электронно-цифровое отображение следов, проистекающее в памяти электронных носителей компьютерной информации, каналах связи

передачи информации, информационно-телекоммуникационных сетях, информационных системах¹.

Киберпространство, включая сеть Интернет, образуется совокупностью компьютерных сетей в транснациональном масштабе, объединенных протоколом TCP/IP, который помечает подключенный к нему сервер или компьютер в виде числового ряда 111.111.111.111. Этот числовой ряд именуется IP-адресом компьютера, имеющего возможность подключаться к сети, получать и предоставлять уникальные идентификационные сведения о себе. Благодаря уникальности IP-адреса представляется возможным найти, получить и передать информацию от одного компьютера (узла) к другому без ошибки адресата. Важным свойством IP-адреса является его скрытый от пользователя характер.

Рассмотрим механизм следообразования при неправомерном доступе к компьютерной информации. Этот механизм включает три основные стадии:

1) материальное проявление признаков следообразующих объектов (в частности, цифровой набор данных, изображение, звук); 2) аналогово-цифровое преобразование, то есть преобразование первичной физической формы выражения следообразующего объекта в цифровую форму; 3) предварительная обработка, передача и сохранение информации в электронно-цифровой форме².

Следует обратить внимание на то, что предварительная обработка информации подразумевает ее преобразование в вид, наиболее пригодный для ее последующего хранения (передачи). Например, посредством уменьшения объем передаваемой (записываемой) информации, повышения

¹ Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. ... канд. юрид. наук. – М., 2018. – С. 47.

² Давыдов В.О., Малахвей Е.Д. О некоторых аспектах криминалистической характеристики преступлений, связанных с неправомерным доступом к компьютерной информации // Известия Тульского государственного университета. Экономические и юридические науки. – 2019. – № 2. – С. 98.

информационной защищенности «запутыванием» алгоритма, шифрованием.

На наш взгляд, при неправомерном доступе к компьютерной информации начальный этап процесса следообразования связан с компьютером киберпреступника, а завершающий – с компьютером жертвы, где наступают последствия, предусмотренные ст. 272 УК РФ. В обозначенной цепи в качестве промежуточных звеньев, на которых остаются электронно-цифровые следы, выступают: сервер провайдера; компьютеры, выполняющие роль посредников при передаче данных; пакеты данных (шлюзы), через которые транслируется информация в электронно-цифровой форме.

У провайдера, предоставившего киберпреступнику выход в Интернет, хранится информация о сетевых подключениях в виде логов, в том числе совершенных с компьютера злоумышленника¹. На сервере провайдера сохраняются: логин и пароль, то есть регистрационные данные для сетевого подключения; электронный адрес компьютера (логический адрес); информация об отправленных (полученных) пакетах информации, времени их отправления (принятия), типе и размере информации, IP-адресах компьютеров отправителя (получателя).

При неправомерном доступе электронно-цифровые следы отображаются в log-файлах. Лог-файлы в любом случае могут содержать ценную идентификационную и справочную информацию, которая позволяет следователю разрабатывать версии о поиске электронно-цифровых следов преступления, совершенного в киберпространстве.

При совершении киберпреступлений электронно-цифровые следы остаются и на машинных носителях компьютерной информации, в частности: изменения файловой структуры, системных областей носителей

¹ Дёмин К.Е. Об методических основах получения криминалистически значимой информации, содержащейся в электронных носителях данных // Вестник Московского университета МВД России. – 2018. – № 4. – С. 45.

информации, постоянной энергонезависимой памяти; изменения настроек компьютерного устройства и отдельных компьютерных программ; нарушения работы компьютера и программ, которые на нем установлены; воздействия на конфиденциальную компьютерную информацию, ее защиты; проявления работы вредоносных компьютерных программ.

Подводя итог, можно сделать следующие выводы:

1. Киберпространство – это область взаимодействия средств компьютерной техники, компьютерных систем (сетей), компьютерных программ пользователей, а также данные, циркулирующих в этих элементах;

2. Электронно-цифровыми следами в кибернетическом пространстве являются отображения изменений любой криминалистически значимой информации относительно ее исходного состояния в области взаимодействия компьютеров, компьютерных систем, глобальных и локальных сетей, в компьютерных программах пользователей, а также в данных, циркулирующих в указанных элементах.

3. Механизм следообразования в киберпространстве представляет собой особую форму протекания процесса, в результате которого происходит электронно-цифровое отображение следов в памяти электронных носителей компьютерной информации, каналах связи передачи информации, информационно-телекоммуникационных сетях, информационных системах. При совершении киберпреступления данный механизм включает три основные стадии:

1) материальное проявление признаков следообразующих объектов (в частности, цифровой набор данных, изображение, звук);

2) преобразование первичной физической формы выражения следообразующего объекта в цифровую форму;

3) предварительная обработка, передача и сохранение информации в электронно-цифровой форме.

2. Деятельность следователя по поиску(обнаружению) и фиксации следов в кибернетическом пространстве

Деятельность по поиску и фиксации следов в кибернетическом пространстве обладает значительной спецификой, обусловленной виртуальной природой самой среды их возникновения и существования. В отличие от традиционных материальных следов, электронно-цифровые следы неосязаемы, легко тиражируемы, модифицируемы и уничтожаемы в считанные секунды, что требует от следователя не только особых технических знаний, но и применения строго регламентированной, научно обоснованной методики работы. Эта деятельность носит комплексный, междисциплинарный характер, сочетающий в себе достижения криминалистики, компьютерных наук и юриспруденции. Ее эффективность напрямую зависит от слаженного взаимодействия следователя со специалистами в области информационной безопасности, программирования и сетевых технологий, чье участие является не просто желательным, а обязательным условием для обеспечения допустимости и достоверности получаемых доказательств.

Локализация электронно-цифровых следов крайне разнообразна и охватывает широкий спектр цифровых устройств и сред. Прежде всего, это стационарные и мобильные устройства: персональные компьютеры, ноутбуки, серверы, смартфоны, планшеты, «умные» часы и другие гаджеты, входящие в экосистему «Интернета вещей». Каждое из этих устройств является потенциальным хранилищем огромного массива информации. Далее, это съемные носители информации: жесткие диски (HDD), твердотельные накопители (SSD), USB-флеш-накопители, карты памяти (SD, microSD), а также оптические диски (CD, DVD), которые, несмотря на моральное устаревание, все еще могут использоваться. Особенностью является и сетевое пространство, где следы носят более временный,

«летучий» характер. К ним относится оперативная память (ОЗУ), которая хранит данные только до выключения устройства, но может содержать критически важные сведения: незашифрованные пароли, ключи, активные сеансы связи. Кэш-память различных приложений и браузеров, предназначенная для ускорения работы, также хранит фрагменты истории посещений, файлы cookie, элементы веб-страниц. Наконец, интернет-трафик, проходящий через маршрутизаторы и серверы провайдеров, представляет собой динамический поток данных, фиксация которого позволяет восстановить картину сетевого взаимодействия.

Классификация следов на статические и динамические имеет фундаментальное значение для выбора правильной тактики их обнаружения и изъятия. Статические следы — это информация, хранящаяся на носителях в относительно неизменном виде после того, как событие произошло. Это файлы на жестком диске (документы, изображения, базы данных), записи в системных журналах, метаданные, информация в резервных копиях. Динамические следы, напротив, генерируются и существуют исключительно в реальном времени в процессе работы системы или действий пользователя. Они крайне уязвимы и исчезают при перезагрузке устройства или завершении процесса. К ним относятся: содержимое оперативной памяти; активные сетевые соединения и открытые порты; запущенные процессы и службы; данные о текущих сеансах пользователей; несохраненные документы в буфере обмена или открытых приложениях.

Работа с динамическими следами требует немедленных действий, часто без предварительного отключения устройства, с применением специальных инструментов для их «заморозки» и извлечения, что подчеркивает необходимость присутствия квалифицированного специалиста непосредственно на месте проведения следственного действия.

Для обнаружения статических следов, которые, в отличие от динамических, представляют собой устойчивые отпечатки, сохранившиеся

на носителях информации после завершения события, применяется комплекс специализированных методов криминалистического анализа. Краеугольным камнем этого процесса является анализ файловой системы с использованием мощных программно-аппаратных комплексов и специализированных программ-анализаторов, таких как Autopsy (как открытое решение), EnCase или Forensic Toolkit (FTK). Эти инструменты функционируют не как простые файловые менеджеры, а как глубокие анализаторы, которые проводят полное низкоуровневое сканирование структуры носителя. Их ключевая функция заключается в реконструкции файловой системы, что позволяет выявлять не только активные файлы, но и критически важные для расследования категории данных: удаленные файлы, информацию о которых система помечает как свободное место, но физически данные остаются на диске до момента их перезаписи; скрытые файлы и каталоги, намеренно сконфигурированные пользователем или приложением для сокрытия их присутствия; а также данные, находящиеся в неразмеченных областях диска (unallocated space) — пространстве, которое не принадлежит ни одному из файлов, но может содержать фрагменты ранее удаленных документов, историю браузера, временные файлы и иные артефакты, мигрировавшие в результате фрагментации или сбоя.

Параллельно и часто в связке с анализом файловой системы активно используются программы для восстановления данных, такие как R-Studio, Ontrack EasyRecovery, DMDE или более доступные утилиты типа Recuva. Принцип их работы основан на сигнатурном анализе, когда программа, игнорируя файловую систему, сканирует носитель побайтно в поиске уникальных последовательностей байт (сигнатур), характерных для заголовков определенных типов файлов (например, 'JPEG', 'PDF', 'ZIP'). Это позволяет восстанавливать информацию даже после форматирования носителя или серьезного повреждения файловой системы. Данные программы помогают вернуть не только намеренно удаленную, но и

поврежденную в результате сбоев, вирусных атак или физических дефектов носителя информации, что зачастую позволяет получить доступ к доказательствам, которые преступник считал безвозвратно утраченными.

Отдельное и высокозначимое направление в работе со статическими следами представляет собой анализ метаданных — то есть «данных о данных». Практически каждый цифровой файл, будь то документ, фотография, аудиозапись или электронное письмо, содержит в себе скрытый слой служебной информации, автоматически генерируемой операционной системой и прикладным программным обеспечением. Для документов Microsoft Office это могут быть сведения об авторе, организации, дате создания, общем времени редактирования и именах компьютеров, на которых файл был открыт. Для цифровых фотографий (формат EXIF) метаданные включают модель камеры или смартфона, настройки экспозиции, дату и время съемки, а в случае мобильных устройств — точные координаты GPS, где был сделан снимок. Анализ этих параметров критически важен для установления подлинности файла, верификации алиби, реконструкции хронологии событий и установления связей между различными объектами и лицами. Например, совпадение уникального идентификатора камеры на фотографиях, изъятых у разных подозреваемых, или обнаружение в метаданных документа имени пользователя, фигурирующего в переписке, являются мощными доказательственными аргументами.

Работа с динамическими и сетевыми следами требует принципиально иных подходов по сравнению со статическими следами, поскольку связана с анализом процессов и данных, существующих только в реальном времени и исчезающих при отключении питания устройства. Эти следы характеризуются высокой волатильностью и требуют применения специальных методик, направленных на их оперативную фиксацию и анализ.

Одним из ключевых методов исследования динамических следов является дампинг памяти (memory dumping) — процесс создания полной бинарной копии содержимого оперативной памяти (ОЗУ) в конкретный момент времени. Эта процедура выполняется с помощью специализированного программного обеспечения, такого как Volatility Framework, Belkasoft RAM Capturer или Magnet RAM Capture. После получения дампа памяти проводится его углубленный анализ, который позволяет извлечь ценнейшую информацию: пароли и учетные данные в незашифрованном виде, которые хранятся в памяти активных процессов; ключи шифрования для доступа к зашифрованным дискам и файлам; данные об активных сетевых соединениях и установленных сеансах связи; списки запущенных процессов и загруженных модулей, что особенно важно для выявления следов вредоносного программного обеспечения, которое может не оставлять следов на диске (так называемые fileless-атаки). Анализ памяти также позволяет восстановить фрагменты несохраненных документов, историю буфера обмена и содержимое открытых окон приложений.

Сетевой анализ (network forensics) представляет собой отдельное направление работы, ориентированное на перехват, запись и исследование сетевого трафика. С помощью специализированных аппаратных и программных средств (например, Wireshark, Network Miner, Suricata) осуществляется захват пакетов данных, передаваемых по сети. Последующий анализ этого трафика позволяет: выявлять кибератаки — от сканирования портов до сложных целевых атак; фиксировать факты несанкционированного доступа к информационным ресурсам; обнаруживать передачу конфиденциальных данных за пределы защищенного периметра; устанавливать параметры сетевых соединений (IP-адреса, порты, протоколы), что критически важно для идентификации участников коммуникации и атрибуции инцидента.

Контент-анализ сетевых ресурсов — это метод, который применяется для исследования содержательной стороны информации, размещенной в открытых и закрытых сегментах интернета. Он включает в себя мониторинг и анализ контента на платформах социальных сетей (ВКонтакте, Telegram, Instagram), в блогах, на форумах, а также в специализированных сетях, таких как Darknet (Tor, I2P). Целью анализа является выявление ключевых слов и фраз, связанных с преступной деятельностью; установление смысловых связей между различными субъектами и сообществами; идентификация информации криминального характера — от торговли запрещенными веществами до распространения экстремистских материалов и организации противоправных действий.

Для практической реализации этих методов в отношении мобильных устройств применяются универсальные аппаратно-программные комплексы, такие как Cellebrite UFED, MSAB XRY или отечественный «Мобильный криминалист». Эти решения предназначены для физического и логического извлечения данных с широкого спектра устройств (смартфонов, планшетов, GPS-навигаторов) и позволяют получать не только пользовательские данные (контакты, сообщения, фотографии), но и служебную информацию — журналы вызовов, историю локаций, данные приложений, включая кэшированные и удаленные файлы. Важной особенностью этих комплексов является возможность обхода блокировок устройств и извлечения данных даже с поврежденных носителей.

Обнаруженная в кибернетическом пространстве информация, сколь бы значимой она ни была, сама по себе не обладает доказательственной силой. Её необходимо надлежащим образом зафиксировать, превратив из набора цифровых данных в полноценное юридическое доказательство. Фиксация в криминалистическом понимании — это не просто копирование или сохранение файлов, а целостный удостоверительный процесс, представляющий собой систему последовательных действий

уполномоченного лица (следователя), направленных на закрепление криминалистически значимой информации в строго предусмотренной уголовно-процессуальным законом форме. Главная цель этого процесса — обеспечить допустимость, достоверность и неизменность полученных сведений для их последующего использования в доказывании по уголовному делу.

Процесс фиксации состоит из двух неразрывно связанных и взаимодополняющих составляющих: процессуальной и технико-криминалистической.

Процессуальная составляющая является фундаментальной и обеспечивает юридическую силу доказательству. Она заключается в тщательном и детальном оформлении протоколов соответствующих следственных действий (осмотра места происшествия, выемки, осмотра вещественных доказательств). В протоколе должны быть исчерпывающе отражены все предпринятые действия, последовательность и суть каждого шага, от подключения носителя до запуска специализированного ПО, обстоятельства обнаружения, идентификационные признаки обнаруженных объектов и примененные технические средства.

Только в результате безупречного процессуального оформления, соответствующего требованиям УПК РФ, информация обретает статус допустимого доказательства.

Технико-криминалистическая составляющая обеспечивает наглядность, полноту и объективность фиксации. Она реализуется с помощью различных форм:

1. Графическая форма: Создание планов, схем и чертежей, например, топологии локальной сети, схемы подключения компьютерного оборудования на месте происшествия, что помогает визуализировать сложные взаимосвязи.

2. Предметная форма: непосредственное изъятие и приобщение к делу самих материальных носителей информации (жестких дисков, флеш-накопителей, SIM-карт), которые упаковываются и опечатываются с соблюдением правил, исключающих их повреждение или модификацию.

3. Наглядно-образная форма: наиболее распространенная для цифровой среды, включающая: фото- и видеосъемку; создание скриншотов (снимков экрана): это основной способ фиксации содержимого экрана при работе с программами, браузерами, интерфейсами. К скриншотам предъявляются строгие требования по атрибуции. В колонтитулах или в сопроводительной описи обязательно указывается: полный URL-адрес веб-страницы; точные дата и время фиксации с указанием часового пояса; наименование и версия программного обеспечения (браузера, почтового клиента), с помощью которого осуществлялся просмотр; идентификационные характеристики компьютера, включая его сетевое имя, IP-адрес, MAC-адрес.

В качестве объектов фиксации выступают все виды цифровых артефактов: отдельные файлы и их совокупности; журналы регистрации (логи) системные и прикладные, отражающие хронологию событий; метаданные, извлеченные из файлов; история браузера, кэш и cookie; переписка из мессенджеров, социальных сетей и электронной почты; настройки сетевых подключений и конфигурации программного обеспечения. Каждый из этих объектов фиксируется с применением описанного выше dual-track подхода, сочетающего юридическую корректность протокола и техническую точность прилагаемых материалов. Подводя итог, можно сделать следующие выводы:

1. Деятельность по поиску (обнаружению) следов в кибернетическом пространстве предполагает применение научно обоснованных способов и методов, в частности, такие как распечатка на бумажный носитель информации с монитора; методы обнаружения

статических следов и методы обнаружения динамических следов в киберпространстве; метода анализа данных; «дампинг» памяти; анализ файловой системы; использование программ-шпионов, устанавливаемых на устройстве пользователя; обнаружение и анализ метаданных файлов; метода сетевого анализа. Кроме того, применяются методы цифровой криминалистики, предполагающие применение средств анализа электронно-цифровых данных (программы для восстановления данных, анализаторы жесткого диска), методов сбора и обработки следов о посещении сайтов, кэш-файлов и системных логов.

2. Под фиксацией понимается удостоверительный процесс (система действий), направленный на закрепление уполномоченным лицом криминалистически значимой информации в предусмотренной уголовно-процессуальным законом форме.

3. Тактика производства отдельных следственных действий как средства фиксации доказательственной информации, хранящейся в кибернетическом пространстве

Основными следственными действиями, посредством которых осуществляется легальная и процессуально грамотная фиксация доказательственной информации из киберпространства, являются выемка и осмотр. Эти действия, регламентированные Уголовно-процессуальным кодексом РФ, образуют *procedural backbone* (процессуальный хребет) работы с цифровыми доказательствами, обеспечивая их допустимость для суда.

Выемка электронно-цифровых носителей и информации проводится в ситуациях, когда следователю достоверно и из определенных источников (например, из оперативных данных или показаний) известно точное местонахождение конкретного носителя информации (сервера, ноутбука, смартфона) или требуется получить определенные данные, хранящиеся у конкретного лица или организации. Ее основная императивная цель — изъятие информации без внесения в нее каких-либо изменений, повреждений или уничтожения. Любое неосторожное действие может привести к безвозвратной утрате доказательств, например, срабатыванию механизма шифрования или удалению данных.

На подготовительном этапе производства выемки критически важное значение имеет комплекс организационно-подготовительных мероприятий. Во-первых, является обязательным привлечение специалиста в области информационных технологий, который не просто консультирует, а активно участвует в действии.

Во-вторых, требует внимания подбор понятых. Желательно, чтобы это были лица, обладающие хотя бы базовыми знаниями в области

компьютерной техники, способные не только формально удостоверить факт действий, но и понять их суть.

В-третьих, необходимо заранее обеспечить условия для сохранности данных: подготовить экранированные пакеты (Фарадеевы чехлы) для мобильных устройств, чтобы исключить удаленное стирание, запастись антистатическими пакетами для жестких дисков, специальными контейнерами и средствами для опечатывания. Также на данном этапе решается вопрос о необходимости привлечения сотрудников органов дознания для обеспечения оперативного прикрытия и безопасности.

Непосредственно на месте производства следственного действия реализуется четкий тактический алгоритм, направленный на минимизацию рисков:

1. Немедленный запрет всем присутствующим в помещении прикасаться к любой компьютерной технике, клавиатурам, мышам, мобильным устройствам. Любое касание может запустить деструктивные скрипты или исказить данные в памяти.

2. Детальная фиксация обстановки с помощью фото- и видеосъемки. Особое внимание уделяется схемам подключения кабелей (электропитания, сетевых, периферийных устройств). Рекомендуется снабжать кабели бирками с номерками, а в протоколе отражать их расположение. Это важно для последующей точной реконструкции системы.

3. Если устройство включено, то нельзя его сразу выключать. Необходимо: сделать полноэкранный скриншот для фиксации активных окон, программ, открытых документов; сфотографировать экран под разными углами для исключения искажений; по возможности, со специалистом, провести быстрый "живой" осмотр запущенных процессов (через Диспетчер задач или аналоги) и зафиксировать его результаты.

4. Корректное обесточивание оборудования проводится с участием специалиста. Простое выдергивание шнура из розетки может повредить данные на дисках.

5. Изъятие, маркировка и упаковка производятся с особой тщательностью. Каждый носитель (жесткий диск, флешка, телефон) изымается по отдельности, упаковывается в антистатический пакет, который помещается в жесткий контейнер для предотвращения физических повреждений. На упаковке делается пояснительная надпись и накладывается сургучная печать или специальная пломба, исключающая несанкционированный доступ. В протоколе детально описывается состояние каждого изъятых предмета.

Отдельную процессуальную и тактическую специфику имеет выемка информации у операторов связи и интернет-провайдеров. Такая выемка направлена на получение абонентской информации, детализации соединений, логов доступа, архивов электронной почты и т.д. Ключевая особенность — эта процедура, как правило, требует получения судебного решения (ст. 165 УПК РФ), поскольку затрагивает право на тайну связи. Исключение составляет случай, когда абонент (например, потерпевший) добровольно предоставляет имеющуюся у него информацию или дает письменное согласие на ее истребование. Полученные от провайдера данные (часто на CD/DVD-диске или ином носителе) осматриваются по общим правилам, при этом проверяется целостность упаковки носителя и наличие сопроводительного письма с реквизитами и временными рамками предоставленной информации.

Осмотр места происшествия и цифровых объектов при расследовании преступлений в киберпространстве представляет собой сложное, многоэтапное следственное действие, обладающее значительной процессуальной и тактической спецификой. Его проведение требует от следователя не только общих криминалистических знаний, но и понимания

принципов функционирования цифровых систем, поскольку место происшествия в данном случае носит виртуально-физический дуализм: это и конкретное помещение с технической инфраструктурой, и абстрактное кибернетическое пространство, доступное через эту инфраструктуру.

Важной процессуальной особенностью является то, что осмотр места происшествия, в соответствии с ч. 2 ст. 176 УПК РФ, может проводиться как до, так и после возбуждения уголовного дела. Это позволяет оперативно зафиксировать крайне нестабильную цифровую обстановку, которая может кардинально измениться или быть уничтоженной к моменту формального возбуждения дела. Решение о производстве осмотра до возбуждения дела принимается при наличии явных признаков преступления, требующих немедленного реагирования для сохранения следов.

Первоочередные действия следователя по прибытии на место носят характер неотложных и направлены на "консервацию" цифровой обстановки:

1. Организация охраны места происшествия и удаление всех посторонних лиц. Периметр охраны должен включать не только физическое пространство, но и зону потенциального беспроводного доступа (Wi-Fi), которую, по возможности, следует заблокировать или отключить роутер.

2. Немедленное недопущение любого взаимодействия с техническими устройствами. Объявляется прямой запрет на прикосновение к клавиатурам, мышам, экранам, корпусам компьютеров и серверов, мобильным телефонам.

3. Тщательная фиксация состояния каждого устройства.

4. Проверка наличия и типа сетевых подключений. Визуально и с помощью специалиста определяется, подключены ли устройства к локальной сети (через кабель Ethernet), к интернету (через Wi-Fi-роутер, модем). Фиксируются модели маршрутизаторов, их индикация.

Эффективным тактическим приемом при осмотре является движение «от центра к периферии». В качестве "центра" или отправной точки рассматривается основной узел, генерирующий или хранящий информацию — это может быть центральный сервер, основной рабочий компьютер подозреваемого, маршрутизатор или модем. Именно с их детального осмотра и фиксации начинается работа. После этого осмотр распространяется на периферийные устройства: принтеры, сканеры, внешние жесткие диски, USB-накопители, находящиеся в том же помещении, а затем и на смежные помещения, связанные с "центром" сетью. Такой подход позволяет системно и последовательно документировать всю цифровую экосистему.

Осмотр информации в сети Интернет (веб-сайтов, страниц в социальных сетях, электронной почты) представляет собой виртуальную составляющую осмотра и имеет свою процедуру. Основным способом фиксации является создание скриншотов (снимков экрана). Однако этот процесс должен быть строго регламентирован для придания результатам доказательственной силы. Каждый скриншот сопровождается детальным описанием в протоколе, где указывается: дата и точное время создания снимка; полный URL-адрес просматриваемой страницы; информация об используемом программном обеспечении (браузер, его версия); действия, предшествовавшие созданию снимка (например, "осуществлен вход в учетную запись `socialnetwork.com/user123`"); IP-адрес компьютера, с которого осуществлялся доступ (может быть зафиксирован на самом скриншоте с помощью вспомогательных сайтов, например, `whoer.net`).

Осмотр электронной почты требует особой осторожности и может проводиться двумя основными способами:

1. Через веб-интерфейс (например, Gmail, Mail.ru, Yandex.Почта) в браузере. Это наиболее безопасный способ, так как письма физически остаются на сервере провайдера.

2. С помощью почтовых клиентов (The Bat!, Microsoft Outlook, Mozilla Thunderbird), установленных на изъятом компьютере. Здесь критически важно учитывать настройки протоколов (POP3, IMAP). Протокол POP3 часто настраивается на удаление писем с сервера после их загрузки на компьютер. Поэтому, если осмотр проводится на компьютере подозреваемого, существует риск, что оригиналы писем на сервере уже утрачены. Протокол IMAP более предпочтителен для следствия, так как синхронизирует содержимое между сервером и клиентом, не удаляя письма. Действия следователя при осмотре почты в клиенте должны быть максимально аккуратными, чтобы не изменить метки писем (прочитано/не прочитано), не переместить их по папкам и не запустить автоматические процессы.

Таким образом, осмотр в киберпространстве — это комплексное действие, требующее синхронизации работы по фиксации физической обстановки и виртуальной информации с неукоснительным соблюдением правил, обеспечивающих аутентичность и неизменность цифровых доказательств.

Роль специалиста в процессе обнаружения и фиксации цифровых следов невозможно переоценить, поскольку он выступает основным связующим звеном между технической сущностью цифровых доказательств и процессуальными требованиями уголовного судопроизводства. Его участие не просто желательно, а является объективной необходимостью, обусловленной сложностью и спецификой современных информационных технологий. В отличие от традиционных следов, цифровые артефакты существуют в среде, где некомпетентное действие может привести к их необратимому уничтожению или изменению без возможности восстановления.

Кроме того, специалист осуществляет консультационную функцию по сложным техническим вопросам, возникающим у следователя в

реальном времени. Он разъясняет принципы работы сетевого оборудования, помогает интерпретировать данные системных журналов, поясняет значение тех или иных параметров в настройках программ, рекомендует оптимальную последовательность действий для достижения целей следственного действия. Именно специалист может оперативно предложить альтернативный способ доступа к информации, если первоначальный план оказался невыполним.

К участию в следственных действиях могут и должны привлекаться самые разные эксперты, чья специализация определяется конкретными задачами расследования. Условно их можно разделить на несколько категорий:

1. Сотрудники экспертно-криминалистических подразделений МВД России (ЭКП), которые обладают широкой подготовкой в области компьютерной криминалистики и часто являются будущими исполнителями судебных компьютерно-технических экспертиз по данному уголовному делу. Их участие обеспечивает преемственность между этапом следственных действий и последующим экспертным исследованием.

2. Узкопрофильные технические специалисты:

Специалисты по сетевым технологиям и сетевой архитектуре — для работы с корпоративными сетями, серверами, маршрутизаторами, анализа сетевого трафика.

Специалисты по операционным системам (Windows, Linux, macOS, мобильные ОС Android/iOS) — для глубокого анализа системных артефактов, реестра, журналов событий.

Специалисты по информационной безопасности — для выявления признаков кибератак, анализа вредоносного программного обеспечения, обхода систем защиты.

Специалисты по конкретному прикладному программному обеспечению (например, по бухгалтерским программам, системам управления базами данных, криптографическим средствам).

Сотрудники организаций-провайдеров, которые могут предоставить информацию о технических особенностях работы их сетей и услуг.

Результаты всех проведенных действий с участием специалиста в обязательном порядке подлежат тщательному процессуальному оформлению. Все действия, включая консультации специалиста, его пояснения и манипуляции с техникой, подробно отражаются в протоколе соответствующего следственного действия.

Таким образом, эффективное расследование преступлений, сопряженных с использованием киберпространства, основывается на неразрывной связи и синергии двух фундаментальных компонентов: применения современных технических методов обнаружения цифровых следов, осуществляемого высококвалифицированными специалистами, и строгого, неукоснительного соблюдения процессуальных норм их фиксации в ходе следственных действий, главными из которых являются выемка и осмотр. Пренебрежение любым из этих компонентов — либо техническим, либо процессуальным — неизбежно ведет к утрате доказательственного значения полученной информации, делая бессмысленными все усилия по раскрытию преступления. Следователь и специалист выступают в этом процессе как единая рабочая связка, где первый обеспечивает юридическую корректность, а второй — техническую достоверность.

ЗАКЛЮЧЕНИЕ

В результате проведённой работы были решены поставленные задачи, и сформулированы выводы, приведённые ниже:

Киберпространство — это область взаимодействия средств компьютерной техники, компьютерных систем (сетей), компьютерных программ пользователей, а также данные, циркулирующих в этих элементах;

Электронно-цифровыми следами в кибернетическом пространстве являются отображения изменений любой криминалистически значимой информации относительно ее исходного состояния в области взаимодействия компьютеров, компьютерных систем, глобальных и локальных сетей, в компьютерных программах пользователей, а также в данных, циркулирующих в указанных элементах.

Механизм следообразования в киберпространстве представляет собой особую форму протекания процесса, в результате которого происходит электронно-цифровое отображение следов в памяти электронных носителей компьютерной информации, каналах связи передачи информации, информационно-телекоммуникационных сетях, информационных системах. При совершении киберпреступления данный механизм включает три основные стадии: 1) материальное проявление признаков следообразующих объектов (в частности, цифровой набор данных, изображение, звук); 2) преобразование первичной физической формы выражения следообразующего объекта в цифровую форму; 3) предварительная обработка, передача и сохранение информации в электронно-цифровой форме.

Деятельность по поиску (обнаружению) следов в кибернетическом пространстве предполагает применение научно обоснованных способов и методов, в частности, такие как распечатка на бумажный носитель

информации с монитора; методы обнаружения статических следов и методы обнаружения динамических следов в киберпространстве; метода анализа данных; «дампинг» памяти; анализ файловой системы; использование программ-шпионов, устанавливаемых на устройстве пользователя; обнаружение и анализ метаданных файлов; метода сетевого анализа. Кроме того, применяются методы цифровой криминалистики, предполагающие применение средств анализа электронно-цифровых данных (программы для восстановления данных, анализаторы жесткого диска), методов сбора и обработки следов о посещении сайтов, кэш-файлов и системных логов.

Фиксация электронно-цифровых следов, обнаруженных в кибернетическом пространстве, производится путем составления протокола проводимого следственного действия. с отражением в нем места и обстоятельств обнаружения информации; перечислением обнаруженных объектов с указанием их частных признаков; описанием места хранения информации на носителе; указанием наименования файла, метаданных и атрибутов копируемых файлов, объема файлов; физических характеристик накопителя. К протоколу прилагается графическая составляющая фиксации (иллюстрационные схемы, таблицы, планы, скриншоты).

При производстве выемки должны соблюдаться следующие правила: изъятие компьютерной техники и съемных носителей не должно приводить к изменению информации; при невозможности осмотра электронно-цифровых следов на месте носитель информации должен быть изъят и направлен на экспертизу; все действия в ходе производства выемки должны быть зафиксированы в протоколе следственного действия.

В ходе выемки фиксация доказательственной информации киберпространства должна осуществляться с участием специалиста, в частности, специалиста ЭКП МВД России; специалистов по сетевым технологиям и сетевой архитектуре, по операционным системам и прикладным программам; по средствам связи и телекоммуникациям; программистов или системных программистов и др.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты

1. Уголовный кодекс Российской Федерации : Федеральный закон от 13 июня 1996 г. №63–ФЗ (ред. от 21.04.2025) [Электронный ресурс] // Доступ из справ.-правовой системы «Консультант–Плюс» (дата обращения 03.06. 2025).

2. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174–ФЗ (ред. от 21.04.2025) [Электронный ресурс] // Доступ из справ.-правовой системы «Консультант–Плюс» (дата обращения 03.06.2025).

3. Модельный закон о противодействии киберпреступности (Принят 14.04.2023 в г. Санкт-Петербурге Постановлением 55-20 на 55-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ) // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. – 2023. – № 78 (часть 3).

4. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента РФ от 9 мая 2017 г. № 203 // Собрание законодательства РФ. – 2017. – № 20. – Ст. 2901.

Монографии, научные статьи, диссертации

1. Давыдов В.О., Малахвей Е.Д. О некоторых аспектах криминалистической характеристики преступлений, связанных с неправомерным доступом к компьютерной информации // Известия Тульского государственного университета. – 2019. – № 2. – С. 94–100.

2. Дёмин К.Е. Об методических основах получения криминалистически значимой информации, содержащейся в электронных

носителях данных // Вестник Московского университета МВД России. – 2018. – № 4. – С. 44–47.

3. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. ... канд. юрид. наук. – М., 2018. – 199 с.

4. Мещеряков В.А. Цифровые (виртуальные) следы в криминалистике и уголовном процессе. – URL: <http://www.library.ru/help/docs/n64350/Mesheryakov.pdf> (дата обращения: 20.12.2022).

5. Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук / М. А. Простосердов. – М., 2016. – 232 с.

6. Самойлов А.Ю. Особенности фиксации цифровых следов в ходе проведения следственного осмотра // Академическая мысль. – 2020. – № 2 (11). – С. 96–98.

7. Семикаленова А.И. Цифровые следы: назначение и производство экспертиз // Вестник Университета имени О.Е. Кутафина. – 2019. – № 5. – С. 115–120.

8. Смахтин Е.В. Цифровые технологии и криминалистика: некоторые проблемные аспекты // Российский юридический журнал. – 2018. – № 4. – С. 78–83.

9. Штодина Д.Д. Международно-правовой режим киберпространства : позиция США : дис. ... канд. юрид. наук / Д. Д. Штодина. – Москва, 2023. – 313 с.

10. Яковец Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации : учебное пособие / Е. Н. Яковец. – Москва : Юрлитинформ, 2017. – 406 с.

Ресурсы сети Интернет:

1. Состояние преступности за 2020 – 2025 годы. [Электронный ресурс] – URL: <https://мвд.рф/reports/item/60248328/> (дата обращения: 15.09.2025).

Учебное издание

Евгений Александрович Пидусов

Елена Ивановна Пырьева

Оксана Олеговна Сахно

**Тактика обнаружения, фиксации и изъятия следов, хранящихся
в киберпространстве**

Методические рекомендации

В авторской редакции