Научная статья
УДК 343.98
EDN:TXEAGQ

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Галина Валентиновна ВЕРШИЦКАЯ

vershickaya@yandex.ru, SPIN-код 5178-9904,
https://orcid.org/0009-0006-8689-7438
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Поволжский институт управления имени П.А. Столыпина, Россия, Саратов,

Аннотация. Целью статьи является анализ современной криминалистической ситуации интернет-мошенничества в России, а также рассмотрение проблем выявления, раскрытия и расследования данных преступлений, совершаемых с использованием современных информационных технологий, в том числе искусственного интеллекта.

Методология исследования основана на комплексном подходе к анализу содержания элементов криминалистической характеристики (обстановки, способов совершения, типичных следов, личностей потерпевшего и преступника), что позволяет выработать эффективные меры противодействия кибермошенничеству. Используются всеобщий диалектический метод, общенаучные методы (анализ и синтез, индукция и дедукция, системно-структурный, сравнительный), а также частнонаучные методы (формально-юридический, сравнительно-правовой, исторический).

Результаты исследования заключаются в том, что на основании обобщения следственной практики и анализа научной литературы раскрыты основные способы совершения мошенничества с использованием информационно-телекоммуникационных технологий (фишинг, фарминг, социальная инженерия, дипфейки, наступательный искусственный интеллект), выявлены особенности личности современных кибермошенников и социально-психологические характеристики жертв, а также обозначены возникающие в связи с этим проблемы выявления и расследования данного вида преступлений.

Обсуждение проблемы подтверждает, что частная методика расследования мошенничества, совершенного традиционным способом, требует существенной переработки с учетом специфики виртуальной среды. Кроме того, обсуждаются проблемы, связанные с квалификацией сотрудников правоохранительных органов, участвующих в выявлении, раскрытии и расследовании рассматриваемого вида преступлений, а также с латентностью киберпреступлений, анонимностью трафика и сложностью обнаружения цифровых следов. Предлагается комплекс мероприятий, направленных на повышение профессиональной компетенции следователей, совершенствование законодательства и внедрение современных технологических решений.

В заключении доказывается, что указанные меры способны повысить эффективность раскрытия и расследования преступлений, совершаемых с использованием современных информационных технологий.

Ключевые слова: киберпреступность, интернет-мошенничество, способы совершения мошенничества в сети Интернет, виртуальные следы, искусственный интеллект, дипфейки.

Заявление о конфликте интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования: *Вершицкая Г.В.* Криминалистическая характеристика интернет-мошенничества // Вестник Поволжского института управления. 2026. Т. 26, № 3. С. 99–110. EDN: TXEAGQ

Original article

CRIMINALISTIC CHARACTERISTICS OF INTERNET FRAUD

Galina V. VERSHITSKAYA

vershickaya@yandex.ru, SPIN-код 5178-9904, https://orcid.org/0009-0006-8689-7438 Russian Presidential Academy of National Economy and Public Administration, Povolzhsky Institute of Management named after P.A. Stolypin, Saratov, Russia,

Abstract. The aim of the article is to analyze the modern criminalistic situation of Internet fraud in Russia, as well as to identify the problems of detecting, uncovering and investigating these crimes committed using modern information technologies, including artificial intelligence technologies.

The research methodology is based on an integrated approach to analyzing the content of the elements of criminalistic characteristics (the situation, methods of commission, typical traces, the identity of the victim and the identity of the offender), which makes it possible to develop effective measures to counteract cyber fraud. The study employs the universal dialectical method, general scientific methods (analysis and synthesis, induction and deduction, system-structural, comparative), as well as specific scientific methods (formal-legal, comparative-legal and historical).

The results of the study consist in the fact that, based on a generalization of investigative practice and analysis of scientific literature, the author reveals the main methods of committing fraud using information and telecommunication technologies (phishing, pharming, social engineering, deepfakes, offensive artificial intelligence), identifies the characteristics of the personality of modern cyber fraudsters and the socio-psychological characteristics of victims, and also outlines the resulting problems of detecting and investigating this type of crime.

The discussion of the results substantiates that the private methodology for investigating fraud committed in the traditional way requires significant revision taking into account the specifics of the virtual environment. In addition, the problems related to the qualifications of law enforcement officers involved in the detection, uncovering and investigation of this type of crime are discussed, as well as the latency of cybercrimes, traffic anonymity and the difficulty of detecting digital traces. A set of measures is proposed aimed at improving the professional competence of investigators, improving legislation and implementing modern technological solutions.

The conclusion proves that the indicated measures can contribute to increasing the effectiveness of solving and investigating crimes committed using modern information technologies.

Keywords: cybercrime, Internet fraud, methods of committing fraud on the Internet, virtual traces, artificial intelligence, deepfakes.

Conflicts of interest. The author declares no conflicts of interest.

For citation. *Vershitskaya, G.V.* Criminalistic Characteristics of Internet Fraud // The Bulletin of the Volga Region Institute of Administration. 2026. Vol. 26, № 3. P. 100–110. EDN XEAGQ

Введение. В современном обществе цифровизация всех сфер жизнедеятельности человека стала неотъемлемой частью социального и экономического развития. Однако вместе с положительными эффектами стремительного прогресса информационных технологий наблюдается рост числа преступлений, совершаемых с их использованием. Особое место среди таких деяний занимает интернет-мошенничество — одно из наиболее распространенных и динамично развивающихся проявлений киберпреступности. Именно кибермошенничество представляет собой достаточно актуальную и крайне опасную проблему для всех пользователей Интернета. С развитием информационных технологий и переходом большинства финансовых операций в онлайн-формат киберпреступники находят все более изощренные и усложненные способы совершения интернет-мошенничества. Использование преступниками современных технических средств и анонимных коммуникаций затрудняет выявление, раскрытие и расследование данного вида преступлений. В таких условиях особое значение приобретает формирование научно обоснованной криминалистической характеристики киберпреступлений, включающей совокупность методически важных элементов, способствующих повышению эффективности деятельности правоохранительных органов по противодействию киберпреступности.

Материалы и методы исследования. Методологическую основу исследования составляет комплексный подход к анализу криминалистической характеристики интернет-мошенничества, позволяющий системно рассмотреть его элементы (обстановку, способы, следы, личность потерпевшего и преступника) в их взаимосвязи с современными технологическими реалиями. В работе использован всеобщий диалектический метод для изучения интернет-мошенничества как динамично развивающегося социально-правового явления, осуществляемого в условиях постоянного технического прогресса. Применение общенаучных методов (анализа и синтеза, индукции и дедукции, системно-структурного, сравнительного) позволило выделить и обобщить элементы

криминалистической характеристики, а также сопоставить различные подходы к пониманию личности преступника и способов совершения деяний, представленные в трудах В.А. Аксенова, Т.В. Молчановой, Д.В. Красева, Р.А. Макарова и других авторов. Среди частнонаучных методов использованы формально-юридический для анализа статьи 159.6 Уголовного кодекса РФ, сравнительно-правовой для сопоставления различных подходов к определению искусственного интеллекта (ИИ) и исторический для рассмотрения эволюции понятия ИИ от работы А. Тьюринга до современных интерпретаций.

В качестве материалов исследования использовались нормативно-правовые акты, научные труды отечественных криминалистов, материалы следственной практики, статистические данные МВД России о динамике интернет-мошенничества, а также публикации в средствах массовой информации об актуальных случаях совершения подобных преступлений с использованием технологий ИИ.

Результаты. Криминалистическая характеристика интернет-мошенничества содержит совокупность важной криминалистически значимой информации, характеризующей признаки состава преступления, предусмотренного ст. 159. 6 УК РФ[1], а именно:

— обстановку совершения преступления;

— способ совершения преступления;

— комплекс типичных следов преступления и вероятные места их локализации;

— личность потерпевшего;

— личность преступника.

При рассмотрении обстановки совершения преступления в криминалистическом аспекте следует учитывать совокупность объективных внешних условий и обстоятельств, в которых осуществляется преступная деятельность. Интернет-мошенничество совершается в специфической виртуальной среде, где взаимодействие между преступником и потерпевшим осуществляется посредством информационно-телекоммуникационных технологий. Как правило, это интернет-сайты, социальные сети, мессенджеры, электронная почта, электронные торговые площадки и иные онлайн-платформы, исключающие непосредственный физический контакт между преступником и жертвой. По времени интернет-мошенничество чаще всего совершается в вечерние часы, а также в периоды повышенной

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 17 нояб. 2025 г.; с изм. и доп. от 17 дек. 2025 г.; 1 янв. 2026 г.). URL: https://www.consultant.ru/document/cons_doc_LAW_10699/

активности пользователей сети (во время распродаж, праздничных акций и иных массовых онлайн-событий), когда возрастает эмоциональная восприимчивость граждан.

Важным элементом криминалистической характеристики является социально-психологическая обстановка, в которой совершается преступление. Кибермошенники при общении стремятся вызвать у жертвы различные чувства (страх, доверие, сострадание или жадность), создают видимость официального общения (от имени банка, правоохранительных органов или государственных структур) и вынуждают потерпевшего к поспешным действиям.

Анализ способов совершения интернет-мошенничества подтверждает активное применение информационно-телекоммуникационных технологий, что обеспечивает высокий уровень анонимности исполнителей и создает возможность целенаправленного воздействия на широкий круг потенциальных жертв.

Особенно опасным средством совершения преступлений в виртуальном пространстве является использование возможностей ИИ. Содержание понятия «искусственный интеллект» впервые было определено в 1960 г. английским математиком Аланом Тьюрингом в работе «Может ли машина мыслить?». По его мнению, ИИ представляет собой совокупность программных средств, способных эмулировать человеческие качества в области планирования, решения задач, самообучения и постепенного совершенствования своего функционала на основе накопленной информации [1]. С тех пор развитие человеческой цивилизации претерпело значительные изменения. Одним из основных достижений научно-технического прогресса стало создание новых технологий, снижающих энергозатраты труда человека с помощью ИИ. В связи с этим изменилось и содержание понятия «искусственный интеллект», определяемого специалистами по-разному. Так, А.И. Буравлев и В.М. Ветошкин считают ИИ «объединением (симбиозом) технических и программных средств, способным выполнять некоторые творческие функции в определенной предметной области, которые традиционно считаются прерогативой человека» [2].

К сожалению, в настоящее время ИИ используется не только для облегчения трудовой деятельности, но и в преступных целях. В частности, ИИ применяется для совершения различных видов интернет-мошенничества, среди которых фишинг, фарминг, социальная инженерия, разработка дипфейков, «наступательный искусственный интеллект».

Фишинг — это получение конфиденциальной информации путем обмана [3]. Преступники создают поддельные сайты, внешне похо-

жие на официальные страницы банков, государственных служб или интернет-магазинов, и направляют жертвам письма или сообщения с просьбой перейти по ссылке и ввести личные данные. Таким образом они получают доступ к паролям, реквизитам банковских карт и иным сведениям, которые позволяют совершать хищение денежных средств. По мнению Д.Р. Фатаховой, фарминг — это процедура скрытного перенаправления жертвы на ложный IP-адрес [4].

Социальная инженерия — это использование различных психологических приемов для введения человека в заблуждение [5]. Системы ИИ, в том числе нейросети, анализируют посты, комментарии, фотографии и другие данные из открытых источников (в социальных сетях, на форумах), чтобы выявить интересы, привычки, круг общения и даже эмоциональное состояние потенциальной жертвы. Например, зная, что человек увлекается инвестициями, мошенники могут создать персонализированное предложение о «выгодном вложении», адаптированное под его предпочтения. Чаще всего такие действия направлены на то, чтобы жертва самостоятельно раскрыла секретную информацию или совершила денежный перевод на счет преступников.

Разработка дипфейков представляет собой технологии создания поддельных аудио- или видеоматериалов с помощью ИИ, позволяющих имитировать внешность, мимику и голос реального человека (например, руководителя или родственника) [6]. Большие языковые модели (LLM) создают фишинговые письма, сообщения в мессенджерах и даже сценарии атак, имитируя стиль общения конкретного человека. Такие тексты лишены грамматических ошибок, учитывают корпоративный жаргон и используются для убеждения сотрудников в необходимости перевода денежных средств или генерации откровенных материалов с целью шантажа.

Так называемый «наступательный искусственный интеллект», то есть проведение автоматизированных атак на системы безопасности, которые существенно сокращают время их взлома, расширяют возможности воздействия, тем самым увеличивая шансы на успешное проведение кибермошенничества. Так, преступники с помощью ИИ создают специальные боты для проведения мошеннических операций или разрабатывают алгоритмы обмана на торговых платформах [7].

Помимо перечисленных, широкое распространение получили также мошеннические действия в социальных сетях и мессенджерах. Преступники взламывают аккаунты пользователей и, действуя от их имени, обращаются к знакомым с просьбами о финансовой помощи. Довольно часто создаются фальшивые страницы известных людей или

организаций, через которые распространяются ложные акции, розыгрыши и сборы средств.

Типичные следы интернет-мошенничества представляют собой совокупность электронных, финансовых и иных данных, возникших в связи с событием преступления. Электронные следы имеют признаки как идеальных, так и материальных следов и относятся, по мнению специалистов, к так называемым виртуальным или цифровым следам [8].

К числу основных виртуальных следов относятся переписка между преступником и потерпевшим (сообщения в мессенджерах, социальных сетях, по электронной почте), история посещений веб-ресурсов, а также данные браузеров. Большое значение имеет информация о регистрации и авторизации, использовании доменных имен, IP-адреса, подключениях и иных действиях пользователя в сети. Финансовые следы включают данные о переводах денежных средств, банковских операциях, платежах через электронные кошельки, транзакции с использованием криптовалют, а также чеки, квитанции и выписки по счетам.

Личность потерпевшего при интернет-мошенничестве характеризуется совокупностью социальных, психологических и поведенческих признаков. Р.А. Макаров считает, что криминалистически значимые особенности личности потерпевшего и его поведения позволяют установить фактические обстоятельства события преступления, указывающие на цели и мотивы поведения преступника [9].

Чаще всего жертвами интернет-мошенничества становятся лица молодого и пожилого возраста. По данным МВД, молодежь чаще всего страдает от схем, связанных с инвестициями, онлайн-играми и образовательными порталами[2]. Пожилые люди в силу доверчивости и сострадания становятся жертвами схем, связанных с просьбами о помощи родственникам, социальными выплатами или телефонными звонками «от официальных служб» [10]. Лица с низким уровнем компьютерной и финансовой грамотности чаще поддаются обману, поскольку не умеют проверять достоверность полученной информации в Интернете, распознавать фишинговые сайты и сомнительные электронные письма.

Психологические особенности жертв интернет-мошенников включают доверчивость, внушаемость, импульсивность, стремление к быстрой прибыли и эмоциональную уязвимость. Поведенческие признаки жертв проявляются в использовании простых или одинаковых паролей для разных сервисов, переходе по сомнительным ссылкам, передаче

[2] МВД сообщило о росте числа подростков, ставших жертвами кибермошенников. URL: https://1prime.ru/20250628/moshennikneyi-858987784.html

конфиденциальных данных по просьбе «оператора», совершении предоплаты без проверки продавца и публикации личной информации в открытом доступе.

После совершения преступления реакция жертвы проявляется через эмоциональный шок, страх, тревогу, растерянность и чувство вины, а также в практических действиях: блокировке аккаунтов и карт, попытке восстановить контроль над личными данными, обращении в банки и службы поддержки. Вместе с тем многие потерпевшие не сразу обращаются в правоохранительные органы, а пытаются самостоятельно разобраться в ситуации, что приводит к утрате цифровых доказательств.

Личность преступника, по мнению Ю.М. Антоняна, «представляет собой совокупность интегрированных в ней социально значимых свойств, образовавшихся в процессе многообразных и систематических взаимодействий с другими людьми и делающих в свою очередь ее субъектом деятельности, познания и общения» [11].

В специальной литературе содержатся различные определения особенностей личности современного интернет-мошенника.

В.А. Аксенов и Т.В. Молчанова выделяют три группы интернет-мошенников:

— лица, обладающие специальными знаниями в области информационных технологий;

— лица, имеющие психические заболевания, вызванные компьютерными фобиями;

— профессиональные мошенники с корыстными интересами [12].

Очевидно, что третья группа мошенников наиболее опасна для общества и государства.

Д.В. Красев утверждает, что индивидуальные особенности преступника определяют тип мошенничества, где он «специализируется» [13]. По его мнению, интернет-мошенником является, как правило, мужчина 18—35 лет, городской житель с высшим или средним профессиональным образованием, активно участвующий в закрытых онлайн-форумах со знанием специфической терминологии и жаргона. При этом следует отметить, что квалификация злоумышленников может варьироваться от высококвалифицированных специалистов до дилетантов.

Обсуждение результатов. Криминалистическая характеристика преступлений определенного вида является основой частной методики их расследования [14]. Криминалистическая характеристика интернет-мошенничества свидетельствует о том, что средства и способы совершения данного вида преступлений постоянно развиваются, в связи с

чем правоохранительные органы сталкиваются с определенными трудностями при их выявлении, раскрытии и расследовании.

Сложность противодействия киберпреступности и кибермошенничеству определяется следующими обстоятельствами:

1. *Латентность киберпреступлений.* Количество зарегистрированных случаев кибермошенничества значительно ниже реальных, поскольку жертвы не обращаются в правоохранительные органы из-за недоверия, страха, стыда или непонимания, произошедшего. В связи с этим необходимо информировать население о значимости сообщения о преступлениях и о создании цифровых каналов подачи заявлений. Целесообразно разработать программу психологической поддержки жертв кибермошенничества и систему мотивации для тех, кто оперативно сообщает о преступлениях (например, оперативное восстановление доступа к сервисам или бесплатные консультации по безопасности).

2. *Низкая цифровая грамотность населения.* Жертвы, как правило, не всегда понимают, по какой схеме их обманули, что затрудняет получение от них криминалистически значимой информации. В связи с этим необходимо включать в образовательные программы учебных заведений основы кибербезопасности, а для пожилых людей и представителей малого бизнеса организовывать бесплатные курсы и вебинары с практическими кейсами и симуляциями атак. Следует также разрабатывать памятки и чек-листы (например, «Как распознать фишинг», «Что делать при взломе аккаунта»), распространять их через соцсети и госуслуги, создавать круглосуточную горячую линию и чат-бот с ИИ для консультаций по подозрительным ситуациям. Привлечение блогеров и средств массовой информации также может способствовать популяризации правил цифровой гигиены через любой доступный контент.

3. *Анонимность и анонимизация трафика.* Злоумышленники используют VPN, прокси-серверы, Tor и другие технологии для сокрытия своей личности и местоположения. С целью отслеживания местонахождения и идентификации личности преступника следует развивать технологии анализа трафика (например, методы fingerprinting) для выявления паттернов поведения даже при использовании VPN / Tor, внедрять системы мониторинга даркнета с применением ИИ для раннего обнаружения объявлений о продаже украденных данных или услуг хакеров.

4. *Сложность обнаружения следов.* Виртуальные следы в силу их специфических особенностей легко удаляются или шифруются [15]. С целью своевременного обнаружения цифровых следов, по нашему

мнению, необходимо принять законодательные нормы, обязывающие IT-компании и соцсети сохранять ключевые метаданные (время, IP, хеш-суммы файлов) в течение 3—5 лет, а также разработать универсальную методику собирания цифровых доказательств в соответствии с международными требованиями.

5. *Недостаточная высокая квалификация лиц, участвующих в раскрытии и расследовании интернет-мошенничества.* Современные информационные технологии стремительно развиваются, преступники оперативно осваивают новые средства, программные решения и платформы для совершения и сокрытия противоправных деяний. В таких условиях сотрудники правоохранительных органов должны разбираться в технических особенностях функционирования информационно-телекоммуникационных систем и криптовалют, в технологиях ИИ и механизмах образования цифровых следов. Именно поэтому для повышения эффективности криминалистической деятельности целесообразно наладить системное взаимодействие правоохранительных органов с IT-специалистами, экспертами в области кибербезопасности и цифровой криминалистики. Такое сотрудничество позволит обмениваться актуальными знаниями о современных схемах киберпреступлений, совместно разрабатывать методики их расследования, а также оперативно реагировать на технологические новации, используемые интернет-мошенниками. Кроме того, необходимо регулярно проводить различные обучающие мероприятия, семинары и тренинги, направленные на повышение уровня IT-грамотности сотрудников правоохранительных органов. В рамках таких программ следует рассматривать тактические приемы расследования киберпреступлений, особенности собирания и исследования цифровых доказательств. Важно оснастить правоохранительные органы специальным программным обеспечением для быстрого анализа логов, восстановления удаленных данных и визуализации сетевых событий, создать национальные центры киберкриминалистики с лабораториями для проведения судебной экспертизы в сложных случаях (например, при взломе блокчейн-систем).

Заключение. Таким образом, по результатам исследования можно сделать вывод, что представленная криминалистическая характеристика интернет-мошенничества позволяет разработать эффективную методику расследования подобных преступлений. Комплекс предложенных мер позволит повысить профессиональные компетенции сотрудников правоохранительных органов, а следовательно, эффективность раскрытия и расследования киберпреступлений.

Особое значение в современных условиях приобретает изучение зарубежного опыта противодействия киберпреступности, поскольку в эпоху развития ИИ мошенничество приобретает транснациональный характер, что требует новых подходов и повышения эффективности принимаемых мер.

Список источников

1. *Тьюринг А.М.* Может ли машина мыслить? / под ред. и прим. С.А. Яновской (в приложении – статья Джорджа фон Неймана «Общая и логическая теория автоматов» / пер. и прим. Ю.А. Данилова). М.: URSS: Ленанд, 2016. 110 с.

2. *Буравлев А.И., Ветошкин В.М.* Искусственный интеллект: сущность, принципы работы, области применения // Вооружение и экономика. 2024. № 2 (68). С. 33–42. EDN: BXZLNS

3. *Завьялов А.Н.* Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения // Baikal Research Journal. 2022. Т. 13, № 2. DOI: 10.17150/2411-6262/202213(2).36. EDN: SRVHGS

4. *Фатахова Д.Р.* Мошенничество в сети Интернет // Молодой ученый. 2020. № 49 (339). С. 341–344. EDN: DIWWCH

5. *Сивчук Е.С.* Социальная инженерия как способ мошенничества // Молодой ученый. 2020. № 41 (331). С. 128–130. EDN: TLGZVC

6. *Симонян А.А.* Генеративный искусственный интеллект и DeepFake-технологии как угроза информационной безопасности граждан // Вопросы российского и международного права. 2025. Т. 15, № 2А. С. 165–172. DOI: 10.34670/AR.2025.46.45.017. EDN: QCWLQU

7. *Намиот Д.Е.* О кибератаках с помощью систем искусственного интеллекта // International Journal of Open Information Technologies. 2024. Т. 12, № 9. С. 132–141. EDN: PEEQXY

8. *Вершицкая Г.В.* Возможности использования виртуальных следов в ходе расследования киберпреступлений // Вестник Поволжского института управления. 2022. Т. 22, № 2. С. 17–23. DOI: 10.22394/1682-2358-2022-2-17-23. EDN: LIAQOR

9. *Макаров Р.А.* Личность пострадавшего как элемент криминалистической характеристики хищений, совершенных дистанционно с использованием информационно-телекоммуникационных технологий // Закон и право. 2021. № 11. С. 232–236. DOI: 10.24412/2073-3313-2021-11-232-236. EDN: MDNZPE

10. *Сычева А.В.* Некоторые вопросы криминалистической характеристики «дистанционных» мошенничеств, совершенных в отношении пожилых людей // Вестник Волгоградской академии МВД России. 2022. № 1 (60). С. 135–140. DOI: 10.25724/VAMVD.ZFG. EDN: UGJLAD

11. *Антонян Ю.М.* Личность преступника и исправление осужденных // Вестник РГГУ. Сер.: Экономика. Управление. Право. 2019. № 2. С. 117–127. DOI: 10.28995/2073-6304-2019-2-117-127. EDN: VQWYQG

12. *Аксенов В.А., Молчанова Т.В.* Особенности личности современного интернет-мошенника в механизме индивидуального преступного поведения // Криминологический журнал. 2020. № 4. С. 79–86. DOI: 10.24411/2687-0185-2020-10080. EDN: FBIWJE

13. *Красев Д.В.* Криминологические особенности организованного мошенничества в сфере информационных технологий // Вопросы российского и международного права. 2025. Т. 15, № 3-1. С. 568–575. DOI: 10.34670/AR.2025.13.65.064. EDN: MGDTWE

14. *Таркинский А.И., Магомедов М.Г.* Роль криминалистической характеристики преступлений в формировании методики расследовани // Право и управление. 2024. № 1. С. 274–279. DOI: 10.24412/2224-9133-2024-1-274-279. EDN: PPZAQA

15. *Прокофьева В.А.* Цифровые следы в криминалистике // Управление развитием: экономика, политика, право: сборник научных статей. Саратов: Поволжский институт управления, 2025. С. 75–77. EDN: PMVBAE

Сведения об авторе

ВЕРШИЦКАЯ
Галина Валентиновна,
кандидат юридических наук,
доцент кафедры административного
и уголовного права

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Поволжский институт управления имени П.А. Столыпина, Саратов, Россия,
vershickaya@yandex.ru,
SPIN-код 5178-9904, https://orcid.org/0009-0006-8689-7438

Статья поступила в редакцию
26.01.2026

Одобрена после рецензирования
30.03.2026

Принята к публикации
25.05.2026

The author

Galina V. VERSHITSKAYA,

Candidate of Sciences (Law),
Docent at the Department
of Administrative and Criminal Law

Russian Presidential Academy of National Economy and Public Administration, Povolzhsky Institute of Management named after P.A. Stolypin
Saratov, Russia
vershickaya@yandex.ru,
SPIN-код 5178-9904,
https://orcid.org/0009-0006-8689-7438

The article was submitted
26.01.2026

Approved after reviewing
30.03.2026

Accepted for, publication
25.05.2026