УДК 343.985.7
doi: 10.21685/2072-3016-2025-2-11

Выявление как система действий, формирующих информационную основу расследования преступлений, совершенных с применением цифровых технологий

Р. Н. Подольный

Казанский институт (филиал) Всероссийского государственного университета юстиции (РПА Минюста России), Казань, Россия

podolnyyr01@kznrpa.ru

Аннотация. *Актуальность и цели.* Одной из особенностей расследования преступлений, совершенных с применением цифровых технологий, является то, что оно должно быть не просто быстрым, а стремительным, поскольку преступник всегда предпринимает меры к тому, чтобы после совершения преступления все следы были уничтожены. Для этого преступник использует такие программные продукты, которые ориентированы не только на достижение определенной криминальной цели, но и на уничтожение следов, которые могут указывать на то, что было совершено преступление и к нему причастно определенное лицо. В связи с этим следователь уже на момент начала расследования должен иметь четкий, хорошо продуманный план расследования. Он должен немедля провести первоначальные следственные действия, в результате которых получить максимум доказательств. Это возможно только при условии наличия значительной базы достоверной информации. Поэтому важным является информационная взаимосвязь между деятельностью по выявлению преступлений и деятельностью по их расследованию. Выявление особенностей этой взаимообусловленности является целью данной работы. *Материалы и методы.* Исследование проводилось с использованием системы методов: диалектического материализма и таких общенаучных методов, как метод анализа и синтеза, дедукции и индукции. Применялись специальные криминалистические методы: криминалистического моделирования, системно-деятельностный и ситуационного прогнозирования. Методологическое значение имели разработанные в криминалистике теории и учения, которые были опробованы в практике расследования. *Результаты*. В ходе исследования было установлено, что качество расследования преступлений, совершенных с применением цифровых технологий, зависит от количества и качества информации, полученной при выявлении преступлений названного вида. Большое значение для последующего доказывания имеет оперативно-розыскная информация. *Выводы.* Результаты проведенного исследования позволили сформулировать ряд рекомендаций, касающихся тактики проведения первоначальных следственных действий при расследовании преступлений, совершенных с применением цифровых технологий.

Ключевые слова: преступления, совершенные с применением цифровых технологий, расследование, следственные действия, данные, доказательства

Для цитирования: Подольный Р. Н. Выявление как система действий, формирующих информационную основу расследования преступлений, совершенных с приме-

нением цифровых технологий // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2025. № 2. С. 127–137. doi: 10.21685/2072-3016-2025-2-11

Identification as a system of actions that form the information basis for the investigation of crimes committed using digital technologies

R.N. Podolnyy

Kazan Institute (branch) of the All-Russian State University of Justice (RPA of the Ministry of Justice of Russia), Kazan, Russia

podolnyyr01@kznrpa.ru

Abstract. *Background.* One of the features of the investigation of crimes committed using digital technologies is that it must be not just fast, but rapid, since the criminal always takes measures to ensure that all traces are destroyed after the commission of the crime. To do this, the criminal uses software products that are focused not only on achieving a specific criminal goal, but also on destroying traces that may indicate that a crime has been committed and a certain person is involved in it. In this regard, the investigator must have a clear, well-thought-out investigation plan at the time of the start of the investigation. He must immediately carry out initial investigative actions, as a result of which he will receive maximum evidence. This is possible only if there is a significant database of reliable information. Therefore, the information relationship between crime detection and investigation activities is important. The purpose of this article is to identify the features of this interdependence. *Materials and methods.* The research based on this article was conducted using a system of methods: dialectical materialism and such general scientific methods as the method of analysis and synthesis, deduction and induction. Special forensic methods were used: forensic modeling, system-activity and situational forecasting. The theories and teachings developed in criminology, which were tested in the practice of investigation, were of methodological importance. *Results.* In the course of the study, it was found that the quality of the investigation of crimes committed using digital technologies depends on the quantity and quality of information obtained when detecting crimes of this type. Operational search information is of great importance for subsequent proof. *Conclusions.* The results of the study made it possible to formulate a number of recommendations regarding the tactics of conducting initial investigative actions in the investigation of crimes committed using digital technologies.

Keywords: crimes committed using digital technologies, investigation, investigative actions, data, evidence

For citation: Podolnyy R.N. Identification as a system of actions that form the information basis for the investigation of crimes committed using digital technologies. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Obshchestvennye nauki = University proceedings. Volga region. Social sciences.* 2025;(2):127–137. (In Russ.). doi: 10.21685/2072-3016-2025-2-11

Цифровые технологии – это средство оптимизации человеческой деятельности [1]. Их применение позволяет получить максимально быстро устраивающий использующего его человека результат. Это их свойство способствует тому, что цифровые технологии проникают в самые различные сферы человеческой деятельности. Они используются в производстве товаров и услуг. Они используются в быту, делая его более комфортным. Цифровые

технологии – это уже реальность не завтрашнего, а сегодняшнего дня, поскольку они используются в самых различных сферах деятельности. Привлекательность этих технологий для общества и государства состоит в том, что они позволяют решать социальные проблемы. В частности, благодаря им имеется возможность охвата и вовлечения в социальные проекты значительного числа граждан. Цифровые технологии являются благом, но только тогда, когда они используются во имя его. К сожалению, цифровые технологии могут причинять серьезный вред, если оказываются в руках лиц, готовых идти на преступление ради удовлетворения каких-либо своих интересов. Они могут быть средством достижения преступных целей. Благодаря им может достигаться оптимизация преступной деятельности. Они могут способствовать увеличению причиняемого ущерба. Кроме того, цифровые технологии могут способствовать тому, что совершенное преступление будет невидимым для правоохранительных органов. Тем самым цифровые технологии создают благоприятные условия для того, чтобы виновный в совершении преступления не понес заслуженного наказания. Безнаказанность способствует формированию у преступников убеждения в собственной вседозволенности, что подрывает основы установленного в государстве правопорядка.

Понятие «цифровая технология» в действующем уголовном законодательстве не используется. Это при том, что ни у кого не возникает сомнения в том, что цифровые технологии используются при совершении преступлений, для их оптимизации, для сокрытия следов [2]. Однако это понятие представляет криминалистическую ценность, поскольку позволяет понять особенности того преступления, в котором применялись цифровые технологии, и на основе этого решить вопрос о том, как необходимо расследовать соответствующее преступление. При совершении преступлений с применением цифровых технологий преступник рассчитывает на то, что он сможет уйти от ответственности. Этого он стремится добиться благодаря тому, что цифровая технология позволяет ему действовать анонимно и на расстоянии. Для того чтобы совершить посягательство на жертву, цифровые технологии позволяют не входить в контакт с ней. Они же делают такой контакт невидимым для окружающих, что сокращает вероятность того, что при расследовании можно выявить очевидцев преступления, которые смогут дать показания о существе совершенных преступных действий. Также особенностью цифровых технологий является то, что их применение часто не явно, т.е. достаточно сложно обнаружить следы, указывающие на то, что преступление было совершено. Это тем более сложно, что при применении некоторых технологий преступники вносят в них определенные новации, которые позволяют скрыть следы совершенного преступления. Все это делает применение цифровых технологий привлекательным для преступников. Они уже при планировании преступления предпринимают все для того, чтобы оно не было выявлено, чтобы причиненный вред выглядел как результат сложившихся неблагоприятных обстоятельств.

Особенностью наиболее инновационных цифровых технологий является то, что злоумышленнику необходимо лишь их запустить, все остальное будет сделано без него [3]. К примеру, преступник может сбросить обманным путем такой программный продукт, который сам сможет взломать пароли и перевести денежные средства на соответствующие счета. В таком преступлении сам преступник, по существу, совершает только одно действие – забрасывает вредоносную программу на компьютер жертвы, с которого она управляет своими финансами. Данная вредоносная программа все остальное делает сама. Сама жертва сразу может и не узнать о факте совершения преступления. Тем более она может не знать о том, как соответствующее программное вредоносное приложение оказалось у нее на мобильном телефоне или в компьютере. В связи с этим при расследовании возникают трудности при определении круга лиц, которые могут быть причастными к совершенному преступлению. Потерпевший при совершении в отношении него таких посягательств часто затрудняется сообщить данные, которые способны позволить установить значимые обстоятельства совершения преступления, а также обстоятельства, указывающие на действительного виновника этих преступных деяний. Складывается парадоксальная ситуация, когда потерпевший не может сообщить о механизме совершенного в отношении него преступления. Причиной этого является то, что потерпевший не видит этого механизма, он скрыт и от него. Единственное, что он может увидеть, – это результат в виде причиненного ему ущерба. При этом в отдельных случаях ущерб еще необходимо потерпевшему осознать как результат совершенного преступления, а не результат собственных действий, совершенных в условиях риска.

Используемые злоумышленником для совершения преступления вредоносные программы ориентированы не только на то, чтобы никто не мог увидеть механизма их действия, но и на то, чтобы не оставалось следов. Для этого часто используются программы, которые после достижения преступной цели уничтожают следы своей работы [4]. Кроме того, сами эти программы могут самоликвидироваться, что затрудняет в последующем установление того, что вообще такая программа была. В результате на начальном этапе расследования формируется ситуация информационной неопределенности, когда следователь сталкивается с вопросом: было ли преступление? Этот вопрос усугубляется тем, что потерпевшим от таких преступлений могут являться лица, не имеющие достаточных знаний в сфере цифровой информации, а потому не могущие правильно оценить те действия, которые они сами совершали. Им сложно воссоздать даже свои действия, которые могли способствовать причинению им вреда. По этой причине даже при наличии вреда жертва далеко не всегда сообщает о совершении в отношении себя преступления. Она может оставаться в неведении и считать, что вред был причинен ее необдуманными случайными действиями. Поэтому правоохранительные органы в таких случаях остаются в неведении относительно совершения преступления. Злоумышленники всегда это понимают и стремятся к тому, чтобы использовать отсутствие необходимых знаний у жертвы для того, чтобы

не только добиться поставленной цели, но и скрыть уличающие следы. В связи с этим встает проблема выявления события совершения преступления. Жертва понимает, что ее обманули, значительно позже, как правило после того, как обратится в соответствующую финансовую организацию, в которой у нее открыт счет, с которого были незаконно похищены денежные средства.

Для расследования важным является то, насколько умело и полно была получена и закреплена информация в ходе выявления соответствующего преступления, которое было совершено с применением цифровых технологий. Это обусловлено тем, что на момент начала расследования следователю необходимо знать, в каком направлении вести поисковую деятельность, что необходимо устанавливать. Недопустимо, чтобы было упущено время и не были выявлены и закреплены следы и информация, которые могут иметь изобличающее значение. Важно уже на момент расследования, чтобы следователь знал, какие процессуальные действия ему необходимо выполнить для того, чтобы не было упущенным время, и благодаря этому добиться успеха расследования – установить обстоятельства совершения преступления. Но для этого необходима информация. Данная информация еще не является доказательственной, но она используется при выявлении преступления. В том случае, если ее объем достаточный, то она может быть трансформирована посредством проведения следственных действий в доказательства. Следователь имеет возможность благодаря такой информации воссоздать отдельные обстоятельства совершенного деяния, благодаря чему выдвинуть наиболее вероятную версию. Это, в свою очередь, позволяет определить задачи, встающие перед расследованием, и те следственные действия, проведением которых имеется возможность получить доказательства.

Выявление может осуществляться как посредством проведения следственных действий, так и посредством оперативно-розыскных мероприятий [5]. Посредством проведения следственных действий выявление обстоятельств совершения преступления осуществляется в тех случаях, когда возбуждено уголовное дело. Это, как правило, бывает тогда, когда при расследовании одного преступления благодаря проведению отдельных следственных действий становится известно, что было совершено также и другое преступление. Выявление посредством оперативно-розыскных мероприятий проводится в тех случаях, когда уголовного дела не возбуждалось. В этих случаях оперативно-розыскные мероприятия становятся источником информации, которая позволяет выявить факт совершения преступления. Данный источник имеет значение не только для принятия следователем тактических решений о проведении следственных действий и о порядке их выполнения, но и для принятия некоторых процессуальных решений. В частности, в ч. 1 ст. 144 Уголовно-процессуального кодекса Российской Федерации (УПК РФ) прямо указано на то, что следователь при проверке сообщения о совершении преступления вправе давать письменное поручение о проведении оперативно-розыскных мероприятий органу дознания. Из этого следует то, что оперативно-розыскная информация имеет значение для принятия процессуальных ре-

шений. Это подтверждается ч. 2 ст. 140 УПК РФ, в соответствии с которой основанием для возбуждения уголовного дела является наличие достаточных данных, указывающих на признаки преступления [6]. В данной норме используется понятие «данные», а не «доказательства», что позволяет отнести к основанию для принятия процессуального решения о возбуждении уголовного дела в том числе и сведения, полученные в результате проведения оперативно-розыскных мероприятий [7]. При выявлении преступлений, совершенных с применением цифровых технологий, данная норма уголовно-процессуального закона особенно важна, поскольку позволяет выстроить эффективный механизм реагирования на совершенное преступление, который состоит в том, что решение о возбуждении уголовного дела может быть принято на основании данных в виде сведений, полученных в результате проведения оперативно-розыскных мероприятий. Таким образом, для начального этапа проводимого расследования данные сведения имеют как тактическое, так и процессуальное решение. Их статус как имеющих процессуальное значение указывает на их значимость для установления обстоятельств совершения конкретного преступления.

Для успеха расследования преступлений, совершенных с применением цифровых технологий, важным является постулат: чем больше данных, полученных в том числе благодаря применению оперативно-розыскных мероприятий, тем больше гарантий того, что расследование завершится успешно, т.е. установлением обстоятельств совершения соответствующего преступного деяния. Однако не менее важно, чтобы данные были достоверными. Достоверность – это качество информации, которое позволяет восстановить картину преступления, соответствующую реально имевшему место событию. Есть предубеждение к результатам оперативно-розыскных мероприятий в части их достоверности. И теоретики, и практики часто полагают, что результаты оперативно-розыскной деятельности уже по определению не могут быть настолько же достоверными, как доказательства, которые получены в результате проведения следственных действий. На самом деле это не так. Хорошо известно, что показания могут оказаться ложными, поскольку лицо, которое их дало, может намеренно исказить информацию ради того, чтобы уголовную ответственность не нес определенный человек, который, возможно, является истинным виновным в причинении вреда. В то же время полученные в ходе проведения оперативно-розыскного мероприятия сведения могут в последующем подтвердиться собранными доказательствами и максимально соответствовать действительно имевшим место обстоятельствам совершения преступного деяния. Поэтому данные, полученные в результате проведения оперативно-розыскных мероприятий, могут быть не менее ценными для установления обстоятельств совершенного преступления. Важным здесь является то, что необходимо эти данные подкрепить доказательствами.

При наличии достаточного объема данных, полученных в результате проведения оперативно-розыскных мероприятий, следователь имеет возможность еще на стадии возбуждения уголовного дела определить тактику про-

цессуальных действий, которая обеспечит получение доказательств в количестве, достаточном для убедительного обоснования наличия события преступления и причастности к нему соответствующего лица. Особенностью расследования преступлений, совершенных с применением цифровых технологий, является то, что в качестве его основы являются данные, полученные в результате применения оперативно-розыскных мероприятий. Эти данные должны отличаться высокой степенью достоверности и их количество должно быть достаточным для того, чтобы можно было делать вывод о том, какое событие имело место в действительности. На момент начала расследования преступлений, совершенных с применением цифровых технологий, следователю уже необходимо точно знать, какая тактика способна принести успех, обеспечив создание качественной системы доказательств, уличающей конкретное виновное лицо. Это важно, поскольку промедление в определении тактики может обернуться утратой значимых для расследования данных, в том числе и доказательств. Необходимо, чтобы на момент начала расследования данных преступлений избежать проблем, связанных с информационной неопределенностью, когда нельзя сделать однозначного вывода об отдельных наиболее значимых обстоятельствах. В связи с этим выявление данных преступлений должно рассматриваться в рамках единой методики расследования. Выявление создает предпосылки к тому, чтобы начальная ситуация расследования названных преступлений обладала качеством информационной определенности.

Среди первоочередных задач начального этапа расследования преступлений, совершенных с применением цифровых технологий, является выявление и закрепление доказательств, которые уличают в виновности конкретное лицо. В частности, важно выявление цифровых следов на соответствующем электронном устройстве, с помощью которого совершалось преступление. По этой причине уже на момент начала расследования следователь должен знать, что это за устройство и где оно находится. Поэтому одним из первоначальных следственных действий должно быть изъятие названного устройства с целью выявления соответствующих следов, подтверждающих, что с его помощью совершались преступные действия. Благодаря этому следственному действию имеется возможность получить необходимые уличающие доказательства. Но для этого необходимо, чтобы данное следственное действие проводилось внезапно для лица, у которого производится изъятие [8]. Это предотвратит возможность уничтожения цифровых следов и самого электронного устройства, которое использовалось для совершения преступления. После изъятия важно максимально тщательно осмотреть данное электронное устройство для того, чтобы выявить все следы, которые могут иметь уличающее значение [9]. Изъятие и осмотр электронных носителей информации должны производиться с участием специалиста. Его участие важно для того, чтобы выявить все те цифровые следы, которые могут следователю помочь в установлении обстоятельств совершенного преступления [10]. Кроме того, специалист может оказать следователю помощь в предотвращении действий,

которыми можно причинить вред соответствующему электронному носителю информации. Необходимость участия специалиста продиктована не только интересами тактики расследования, но и требованиями ч. 2 ст. 164.1 УПК РФ.

Задачей, которая стоит при проведении изъятия электронного носителя информации и его последующего осмотра, является формирование следственной ситуации, когда следователь обладает максимально возможным объемом доказательств и информации, с помощью которой можно установить виновное лицо. Успех этих следственных действий во многом зависит от того, насколько значительный объем информации будет получен в ходе выявления соответствующего преступления. В связи с этим важно, чтобы тактика выявления преступления была ориентирована не только на то, чтобы получить данные о совершении преступления, но и на то, чтобы этих данных было достаточно и чтобы они отвечали требованиям достоверности. Таким образом, качество расследования во многом находится в зависимости от тактики выявления преступлений рассматриваемого вида. При этом важно, чтобы и в ходе последующего расследования этих преступлений имело место взаимодействие следователя с органами, осуществляющими оперативно-розыскную деятельность. Это необходимо для того, чтобы предотвратить возможность противодействия расследованию со стороны лиц, которые не заинтересованы в установлении истины. Данное взаимодействие должно быть средством получения следователем информации о том, насколько эффективными являются совершаемые им действия. Такая информация позволяет корректировать проводимое расследование, повышая его результативность.

Среди первоначальных следственных действий при расследовании преступлений, совершенных с применением цифровых технологий, должен быть также допрос лица, у которого был изъят соответствующий носитель электронной информации. При этом статус данного лица, должен устанавливаться следователем исходя из имеющихся у него данных. Это может быть как лицо, подозреваемое в совершении преступления, так и лицо, которое лишь хранило соответствующее электронное устройство, не зная о его причастности к совершенному преступлению. В первом случае данное лицо допрашивается в качестве подозреваемого, во втором – в качестве свидетеля. Следует отметить то, что, как правило, лица, у которых изымается электронное устройство, виновны в совершении соответствующего преступления либо как-то к нему причастны. Для определения статуса лица, которое следует установить, необходимо хотя бы примерное, вероятное знание о том, какое отношение оно имеет к совершенному преступлению. Это возможно установить только при наличии соответствующих данных. С учетом того, что расследование только началось, а медлить с допросом нельзя, это данные, которые следователь получает от органов, осуществляющих оперативно-розыскную деятельность. Поэтому для расследования важны все те данные, которые были получены в ходе деятельности по выявлению конкретного преступления, совершенного с применением цифровых технологий.

Выявление факта совершения преступления, совершенного с применением цифровых технологий, необходимо рассматривать не просто как обычный сигнал, реакцией на который должна быть основательная его проверка посредством проведения процессуальных действий в рамках стадии возбуждения уголовного дела, но и как совокупность оперативно-розыскных мероприятий и иных действий, являющихся источником данных, которые можно использовать для формирования системы доказательств, способной изобличить виновное лицо. В связи с этим выявление преступления необходимо рассматривать не только как деятельность, предваряющую процесс расследования, но и как деятельность, в ходе которой формируется информационная база, необходимая для принятия тактических решений в ходе расследования, которая позволяет сформировать систему доказательств.

Список литературы

1. Бигалиева Я. Г., Плутенко Д. С. Понятие цифровых технологий и их значение в гражданском праве // Право и управление. 2024. № 5. С. 535–540.
2. Матвеев И. В. Взаимовлияние цифровых технологий и уголовного права // Закон и право. 2024. № 7. С. 179–182.
3. Антонова Е. Ю. Механизм совершения преступлений в эпоху цифровизации // Право и государство: теория и практика. 2024. № 1 (229). С. 236–239.
4. Усачев С. И., Усачева Е. А. Информационно-коммуникационные технологии в механизме преступной деятельности // Сибирский юридический вестник. 2024. № 3 (106). С. 110–117.
5. Фомина Е. Н. Особенности оперативного поиска в сети Интернет при выявлении преступлений, совершаемых с использованием информационно-коммуникационных технологий // Деятельность оперативных подразделений: теория и практика : материалы межвуз. науч.-практ. конф. / сост. А. Г. Гришин. СПб. : СПб ун-т МВД России, 2022. С. 161–166.
6. Клещев С. В. Проблемы и перспективы правоприменения отдельных способов проверки сообщения о преступлении // Бизнес. Образование. Право. 2022. № 3 (60). С. 247–252.
7. Махтюк С. О. К вопросу о достаточности доказательств, оснований и данных в уголовном процессе // Российский следователь. 2022. № 2. С. 31–35.
8. Абсатаров Р. Р. Правовые проблемы изъятия электронных носителей информации и получения копий с них // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2023. № 1 (71). С. 25–28.
9. Павлов Е. Н. Особенности методики изъятия электронных носителей информации // Актуальные проблемы противодействия преступлениям экономической и коррупционной направленности : сб. науч. ст. по итогам вузов. науч.-практ. семинара (г. Нижний Новгород, 25 апреля 2023 г.). Н. Новгород : Нижегородская акад. МВД России, 2023. С. 126–130.
10. Кардашевская М. В. Осмотр электронных носителей и изъятие с них криминалистически значимой информации // Судебная экспертиза и исследования. 2022. № 1. С. 79–81.

References

1. Bigalieva Ya.G., Plutenko D.S. The concept of digital technologies and their importance in civil law. *Pravo i upravlenie = Law and management*. 2024;(5):535–540. (In Russ.)
2. Matveev I.V. The Interaction of Digital Technologies and Criminal Law. *Zakon i parvo = Law and rights*. 2024;(7):179–182. (In Russ.)
3. Antonova E.Yu. The mechanism of committing crimes in the digital age. *Pravo i gosudarstvo: teoriya i praktika = Law and state: theory and practice*. 2024;(1):236–239. (In Russ.)
4. Usachev S.I., Usacheva E.A. Information and communication technologies in the mechanism of criminal activity. *Sibirskiy yuridicheskiy vestnik = Siberian juridical journal*. 2024;(3):110–117. (In Russ.)
5. Fomina E.N. Features of operational search on the Internet in identifying crimes committed using information and communication technologies. *Deyatel'nost' operativnykh podrazdeleniy: teoriya i praktika: materialy mezhvuz. nauch.-prakt. konf. = Activities of operational units: theory and practice: proceedings of interuniversity scientific and practical conference*. Saint Petersburg: SPb un-t MVD Rossii, 2022:161–166. (In Russ.)
6. Kleshchev S.V. Problems and prospects of law enforcement of certain methods of verifying a crime report. *Biznes. Obrazovanie. Pravo = Business*. Education. Law. 2022;(3):247–252. (In Russ.)
7. Makhtyuk S.O. On the issue of sufficiency of evidence, grounds and data in criminal proceedings. *Rossiyskiy sledovatel' = Russian investigator*. 2022;(2):31–35. (In Russ.)
8. Absatarov R.R. Legal issues of seizure of electronic information carriers and obtaining copies from them. *Vestnik Kaliningradskogo filiala Sankt-Peterburgskogo universiteta MVD Rossii = Bulletin of the Kaliningrad branch of the Saint Petersburg University of the Ministry of Internal Affairs of Russia*. 2023;(1):25–28. (In Russ.)
9. Pavlov E.N. Features of the methodology for the seizure of electronic information carriers. *Aktual'nye problemy protivodeystviya prestupleniyam ekonomicheskoy i korruptsionnoy napravlennosti: sb. nauch. st. po itogam vuzov. nauch.-prakt. seminara (g. Nizhniy Novgorod, 25 aprelya 2023 g.) = Current issues in combating economic and corruption-related crimes: proceedings of university scientific and practical seminar (Nizhny Novgorod, April 25, 2023)*. Nizhniy Novgorod: Nizhegorodskaya akad. MVD Rossii, 2023:126–130. (In Russ.)
10. Kardashevskaya M.V. Inspection of electronic media and extraction of forensically significant information from them. *Sudebnaya ekspertiza i issledovaniya = Forensic examination and research*. 2022;(1):79–81. (In Russ.)

Информация об авторах / Information about the authors

Роман Николаевич Подольный
преподаватель, Казанский институт (филиал) Всероссийского государственного университета юстиции (РПА Минюста России) (Россия, г. Казань, ул. Фатыха Амирхана, 14)

Roman N. Podolnyy
Lecturer, Kazan Institute (branch) of the All-Russian State University of Justice (RPA of the Ministry of Justice of Russia) (14 Fatykha Amirkhana street, Kazan, Russia)

E-mail: podolnyyr01@kznrpa.ru

Автор заявляет об отсутствии конфликта интересов / The author declares no conflicts of interests.

Поступила в редакцию / Received 18.04.2025

Поступила после рецензирования и доработки / Revised 05.05.2025

Принята к публикации / Accepted 22.05.2025