УДК 343.985.7
МРНТИ 10.85.51

Д.В. Воеводкин
Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Косшы, Республика Казахстан

О СЛЕДОВОЙ КАРТИНЕ ПОДДЕЛКИ ДОКУМЕНТОВ В СФЕРЕ МЕДИЦИНСКОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ

Аннотация. В статье рассмотрены особенности следовой картины преступлений, связанных с подделкой документов в сфере медицинского обслуживания населения, как самостоятельных элементов криминалистической характеристики.

С учетом развития криминалистической техники на современном этапе научно-технической революции, сопровождающейся информатизацией и технизацией преступности, обусловленной интеграцией современных информационных технологий во всех сферах человеческой деятельности, особое внимание обращено на механизм образования таких относительно новых видов следов, как цифровые следы, при расследовании рассматриваемой разновидности преступлений. Проанализированы научные подходы ученых к понятию «цифровых следов», выражена позиция автора относительно данной дефиниции, рассмотрены разновидности «цифровой следовой информации» и их источники.

Даны практические рекомендации по использованию выделенных особенностей при расследовании преступлений, связанных с фальсификацией документов в сфере медицинского обслуживания населения.

Ключевые слова: исследование документов; криминалистическая характеристика; медицинские документы; подделка; следовая картина; следы преступления; фальсификация; цифровые следы.

Д.В. Воеводкин
Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы, Қосшы қ., Қазақстан Республикасы

ХАЛЫҚҚА МЕДИЦИНАЛЫҚ ҚЫЗМЕТ КӨРСЕТУ САЛАСЫНДАҒЫ ҚҰЖАТТАРДЫ ҚОЛДАН ЖАСАУДЫҢ ІЗІ ТУРАЛЫ

Аннотация. Мақалада сот-медициналық сипаттаманың тәуелсіз элементтері ретінде халыққа медициналық қызмет көрсету саласындағы құжаттарды қолдан жасаумен байланысты қылмыстардың іздік көрінісінің ерекшеліктері қарастырылған.

Ғылыми-техникалық революцияның қазіргі кезеңіндегі криминалистикалық техниканың дамуын ескере отырып, қазіргі заманғы ақпараттық технологиялардың адам қызметінің барлық салаларында интеграциялануына байланысты ақпараттандыру мен қылмысты техникаландырумен қатар, қарастырылып отырған қылмыс түрін тергеу кезінде цифрлық іздер сияқты салыстырмалы түрде жаңа іздердің пайда болу механизміне ерекше назар аударылады. Ғалымдардың «цифрлық іздер» ұғымына ғылыми көзқарастары талданды, автордың осы анықтамаға қатысты ұстанымы білдірілді, «цифрлық іздік ақпараттың» түрлері және олардың көздері қарастырылды.

Халыққамедициналық қызметкөрсетусаласындағықұжаттарды бұрмалауменбайланысты қылмыстарды тергеу кезінде бөлінген ерекшеліктерді пайдалану бойынша практикалық ұсынымдар берілді.

Түйінді сөздер: құжаттарды зерттеу; сот-медициналық сипаттама; медициналық құжаттар; жалғандық; іздік сурет; қылмыс іздері; жалғандық; сандық іздер.

D.V. Voevodkin
The Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Kosshy c., the Republic of Kazakhstan

ABOUT THE TRACE PATTERN OF FORGERY OF DOCUMENTS IN THE FIELD OF MEDICAL CARE OF THE POPULATION

Abstract. The article considers the features of the trace pattern of crimes related to forgery of documents in the field of medical care of the population as independent elements of criminalistic characteristics. The article analyzes the natural features inherent in the considered type of crimes and influencing the emergence of the relationship between the methods and mechanisms of their commission.

Taking into account the development of forensic technology at the present stage of the scientific and technological revolution, accompanied by informatization and technization of crime, due to the integration of modern information technologies in all spheres of human activity, special attention is paid to the mechanism for detecting and removing such relatively new types of traces as digital traces when investigating the type of crimes under consideration.

Practical recommendations are given on the use of the highlighted features in the investigation of crimes related to the falsification of documents in the field of public health care.

Keywords: document research; forensic characteristics; medical documents; forgery; trace pattern; traces of crime; falsification; digital traces.

DOI: 10.52425/25187252_2023_29_84

Введение. Согласно закону всеобщей взаимосвязи и взаимообусловленности явлений и общего свойства отражения материи, всякое преступление оставляет следы. Взаимосвязь и взаимообусловленность в контексте криминалистики обычно обозначают связь между различными элементами преступления и его следствиями. Это может включать в себя взаимосвязь между злоумышленником, жертвой, методами, используемыми преступником, и следами, оставленными на месте преступления. Исследование этих взаимосвязей может помочь в раскрытии и расследовании преступлений.

Концепция отражения в криминалистике может относиться к процессу интерпретации и анализа доказательств и следов. Этот процесс может быть рассмотрен как «отражение» реальности преступления, поскольку он включает восприятие и понимание информации, которую предоставляют доказательства и следы.

В каждом отдельном случае взаимосвязи и отражения могут быть сложными и зависят от множества факторов, включая природу преступления, обстоятельства, при которых оно было совершено.

Материалы и методы. Основу исследования образуют труды ученых криминалистов, раскрывающих такие элементы криминалистической характеристики как следовая картина совершения преступлений. Методологической основой исследования послужил общий диалектический метод научного познания, носящий универсальный характер, а также методы логической дедукции, индукции, приемы обобщения и описания.

Результаты, обсуждение. Следы, которые в практике часто называют материально зафиксированными отображениями, обычно отражают внешний рельеф объекта, который оказывает воздействие или подвергается воздействию.

Традиционно в криминалистике выделяют следы идеальные («отпечатки» события в сознании людей) и материальные («отпечатки» события на предметах, изменения обстановки события). Отдельными криминалистами предложено выделить следы, оставляемые при совершении преступлений посредством

информационно-коммуникационных технологий. В юридической литературе данные специфические следы именуются и определяются по-разному: «виртуальные следы» [1], «информационные следы» [2]; [3], «компьютерные следы» [4], «электронно-цифровые следы» [5], «бинарные следы» [6].

Как можно увидеть из разнообразия представленных определений, сегодня имеет место дискуссия относительно введения их в употребление и использование.

Одними авторами указывается, что виртуальные следы являются исключительно материальными следами, поскольку были зафиксированы на материальных носителях путем изменения свойств или состояния отдельных их элементов [7]. Е.Р. Россинская предлагает именовать такие следы информационно-технологическими.

Другими отмечается, что признаки преступлений, совершаемых с использованием информационных технологий, чаще всего лишены физической формы и обычно проявляются в телекоммуникационных или компьютерных сетях [8].

Существуют и другие точки зрения ученых, подробно останавливаться на которых мы не будем, отметим лишь, что разделяем точку зрения Е.Р. Россинской о материальной природе таких следов.

Вместе с тем, полагаем, что более верным для таких следов было бы «электронно-цифровые», под которыми понимают «любую криминалистически значимую компьютерную информацию, то есть сведения (сообщения, данные), которые находятся в электронно-цифровой форме и зафиксированы на материальном носителе с помощью электромагнитных взаимодействий либо передаются по каналам связи посредством электромагнитных сигналов» [5, 94 стр.].

Позиции материальности рассматриваемой категории следов придерживается и ряд зарубежных ученых [9]; [10].

На наш взгляд, электронно-цифровые следы необходимо рассматривать как один из подвидов материальных следов, наряду с одорологией, и изучать в разделе криминалистической техники, либо в новой подотрасли криминалистики, именуемой «цифровой», понятие которой введено в употребление некоторыми учеными, в том числе в странах запада [11]; [12] (digital forensic); [13]; [14]. На наш взгляд, данный термин имеет право на существование, поскольку отражает существенные изменения в природе и характере преступности, которые произошли в результате широкого распространения цифровых технологий и интернета. Однако целесообразно рассматривать его как часть криминалистики, специализированную в информационной и компьютерной области. С формальной точки зрения более уместно говорить не о «цифровой криминалистике», а о «криминалистике в эпоху цифровой трансформации».

Одной из ключевых задач следственно-оперативной группы, работающей на месте производства первоначальных и неотложных следственных действий (например, осмотр места происшествия, выемка, обыск), является обнаружение, документирование и изъятие следов, которые указывают на способ совершения преступлений, связанных с подделкой медицинских документов в сфере медицинского обслуживания населения. Следует отметить, что учитывая характер таких преступлений, обычно на месте преступления можно обнаружить следующие категории следов, связанные с подделкой медицинских документов:

- следы-предметы;
- следы-отображения;
- следы веществ;
- электронно-цифровые следы.

К предметным следам при производстве отдельных следственных действий относятся: непосредственные материальные носители (поддельные документы; подлинные документы с элементами частичной подделки; поддельные элементы документов); оборудование и приспособления (печатные станки, ризографы, принтеры, плоттеры, сканеры, и т.д.); расходные материалы (бумага, картон, клей, краска, тонер и т.п.); документация (отчетность, бухгалтерия, прикрытия). Особое значение получения данных следов

заключается в том, что их дальнейшее наличие в материалах уголовного дела является необходимым элементом признания их в качестве вещественного доказательства при расследовании рассматриваемой разновидности преступлений.

В качестве наиболее распространенных следов отображений по делам, связанным с подделкой документов в сфере медицинского обслуживания населения, выступают следы пальцев рук. Не так часто, но в местах изготовления поддельной продукции могут встречаться и следы обуви. Процесс обнаружения, фиксации и изъятия следов данной группы имеет определенные специфики, поэтому, на наш взгляд, обеспечение работы со следами-отображениями в ходе расследования фальсификации должен осуществлять специалист-криминалист. Например, целесообразно осуществлять поиск следов на следовоспринимающих поверхностях, которые наиболее благоприятны для их фиксации и изъятия. Учитывая, что процесс изготовления поддельной документации сопряжен с использованием различных предметов (бумага, штампы, печати, клавиатура), специалисту-криминалисту необходимо уделить особое внимание данным объектам на предмет наличия на них следов пальцев рук.

Общеизвестно, что благодаря передовым технологиям современной дактилоскопии при помощи изъятых с места происшествия отпечатков пальцев рук появляется возможность установления лиц(а), их оставивших. Характерные особенности, а также количество следов рук и ног позволяет судить о численности лиц, задействованных в процедуре изготовления поддельных документов. Разумеется, деятельность множества людей, осуществляющих подделку документов, не может выпадать из поля зрения специалистов-криминалистов по сбору следовой информации.

Следы-вещества, в отличие от вышеперечисленных групп следов, носят второстепенный характер и используются в качестве объектов, направляемых на экспертное исследование. К ним следует отнести различные порошки, растворы, жидкости, химические соединения.

По устоявшемуся мнению большинства экспертов, цифровые следы типичны для преступлений, связанных со злоупотреблением информационно-коммуникационными технологиями. Однако, в настоящее время они уже составляют значительную часть следов любого преступления, в том числе при подделке документов рассматриваемой разновидности преступлений. По результатам исследований, на самом деле цифровые следы встречаются в 80-90% случаев [15, 199 стр.].

Об этом свидетельствуют и материалы уголовных дел по фактам подделки медицинских документов. Так, из приговора суда №2 города Актобе Актюбинской области от 14.09.2021 года следует, что гражданка М., будучи врачом общей практики медицинского учреждения «М… Ц…», пользуясь своими служебными полномочиями, в кабинете здания медицинского учреждения, используя рабочий компьютер марки «ASUS» и рабочий принтер марки «HP Laser Jet P1102» по шаблонному бланку ТОО «К… О…» с имеющимися заявками иных лиц, ранее официально сдавших заборы анализов для прохождения ПЦР, путем редактирования содержания рядов шаблонов в текстовом редакторе программы «Word» ввела полные анкетные данные лица, которому был необходим поддельный документ, в том числе индивидуальный идентификационный номер, число, месяц и год рождения, а также фиктивное время забора анализов и одобрение заявки от «КДЛ «Олимп». Затем М., заполнив шаблонный бланк ТОО «КДЛ ОЛИМП» на гражданина Б., распечатала файл заполненного шаблонного бланка справки ПЦР с отрицательным результатом на рабочем принтере марки «HP Laser Jet P1102», тем самым изготовила поддельный документ в виде справки ПЦР с отрицательным результатом с последующей ее реализацией за денежное вознаграждение в сумме 7 500 тенге.

В процессе анализа цифровых следов

на начальных стадиях не всегда очевидно, отражают ли эти следы незаконные действия, могут ли они быть применены для криминалистических исследований более широкого масштаба, или это просто обычные следы, которые обычно не рассматриваются как свидетельства преступных действий. Поэтому ответ варьируется в зависимости от того, что является предметом исследования в ходе первоначальных следственных действий. Вне зависимости от ситуации, любые доказательства, связанные с делом, исследовательские гипотезы и рабочие версии следствия должны быть подтверждены или опровергнуты. В связи с этим, как при работе со следами отображениями требуется участие криминалиста, так и для обнаружения и документирования электронно-цифровых следов необходима экспертная поддержка специалиста в области компьютерной техники. При этом, характер преступления будет определять прогноз наличия необходимого оборудования и подготовку наиболее подходящих технических процедур для каждого конкретного случая.

Электронно-цифровые следы, возникающие при подделке документов в сфере медицинского обслуживания населения, представляют собой следы, сохраняющиеся на устройствах хранения информации и отображающие изменения в содержащихся на них данных. Это включает следы изменения информации (баз данных, текстовых файлов, файлов-отчетов и журналов операций, системного реестра, учетных записей пациентов) на различных носителях, таких как жесткие диски компьютеров, лазерные и магнитооптические диски, карты памяти и т.д. Устройства хранения информации могут содержать следы удаления или изменения информации, например, удаление имен файлов из каталогов, стирание или добавление отдельных записей, физическое разрушение или демагнитизация носителей.

Следы информационного воздействия сохраняются на следующих объектах:

- постоянные устройства хранения информации. Это могут быть внешние устройства, такие как диски, флеш-накопители, карты памяти и т.д., а также встроенные жесткие диски компьютера. На этих устройствах следы обычно сохраняются относительно стабильно и могут оставаться на протяжении длительного времени;

- оперативное запоминающее устройство (далее – ОЗУ) или, в обиходе, «оперативная память». Она управляет обработкой файлов во время работы компьютера через нее проходят команды от операционной системы и пользователя. Эта информация является особенно ценной, так как позволяет полностью воссоздать последовательность выполняемых на компьютере информационных процессов, но эти данные могут быть потеряны при выключении устройства;

- оперативная память периферийных устройств, таких как клавиатуры, мониторы, принтеры, сканеры и т.д. Главный процессор компьютера взаимодействует с подключенными к нему устройствами через эти ОЗУ, отправляет им команды и получает от них подтверждение выполнения. В свою очередь, ОЗУ может хранить информацию о проходящих через него данных. Иногда эти ОЗУ могут содержать значительное количество информации в течение длительного времени. Например, ОЗУ современных принтеров способны сохранять документы, отправленные на печать, даже если устройство было временно отключено;

- оперативная память компьютерных устройств связи и сетевых устройств. Компьютеры обмениваются информацией через устройство связи, такое как модем, которое также оснащено своей оперативной памятью для поддержания его функционирования. Через него может проходить информация, отправляемая или получаемая компьютером, и также сохраняться в ОЗУ. Обычно информация в таких ОЗУ не хранится дольше нескольких часов. После выключения компьютера эта информация обычно теряется;

- системы и сети связи (электросвязи), включающие каналы проводной, радио- и оптической связи, а также другие виды каналов;

- мобильные телефоны, персональные цифровые помощники (КПК).

Следующие типы следов могут быть извлечены из упомянутых устройств хранения данных:

- файлы, которые, при законном и регулярном использовании компьютера, было бы невозможно обнаружить в данном месте, или которые были модифицированы каким-либо образом в случае нарушения этого регулярного использования;

- журналы регистрации, включая log-файлы, которые служат отчетами о всех операциях, выполняемых компьютером;

- инструменты для управления и организации электронной информации на компьютере, включая таблицы размещения файлов, системные реестры операционных систем, отдельные кластеры магнитных носителей информации, файлы и каталоги хранения электронной почты, файлы конфигурации программ удаленного доступа и т.д.

Следует иметь в виду, что такие следы могут быть обнаружены не только на персональном компьютере злоумышленника, но и на сервере, посредством которого осуществлялся доступ. Это может включать серверы электронной почты, файловые хранилища, форумы и любые другие места, где возможен обмен информацией либо ее хранение. Кроме того, на компьютере подозреваемого могут быть обнаружены дополнительные следы, например, результаты тестирования использованного злоумышленником программного обеспечения или устройств. Это может включать файлы журналов ошибок, кэш браузера, временные файлы и прочее, которые могут свидетельствовать о деятельности пользователя.

Информация о сообщениях, переданных через Интернет, фиксируется в лог-файлах (текстовый файл, куда автоматически записывается важная информация о работе системы или программы, своеобразный журнал событий). Эти файлы содержат подробности о том, кто инициировал сообщение, когда и в какое время это произошло, и если какие-то файлы были затронуты, то какие именно. Лог-файлы могут предоставить данные об:

- пользователе, включая его имя, адрес, дату рождения, номер телефона, адрес поставщика услуг интернета, электронную почту, идентификаторы любых номеров или счетов, используемых для платежей за услуги интернет-провайдера, идентификационные данные юридического лица, список подписанных или предоставленных услуг, текущий и предыдущий IP-адреса, а также дополнительные адреса электронной почты;

- сообщении, что может включать первоначальный номер телефона, использованный для связи с LOG-файлом, дату и время сеанса связи, статические или динамические IP-адреса, зарегистрированные у провайдера интернет-сервисов и соответствующие телефонные номера, скорость передачи сообщения, информацию об исходящих сеансах связи, включая типы протоколов и используемые протоколы.

Важно заметить, что лог-файлы могут служить ценным источником информации при выяснении в ходе расследования рассматриваемой разновидности преступлений сведений о соучастниках, их ролях и т.п.

При изготовлении поддельных документов зачастую используется сканирование оригинального документа с последующим внесением в него ложных сведений. Практически каждый, кто обладает базовыми навыками работы с простыми графическими редакторами (например, Paint), может подделать отсканированный документ. Это не предполагает знание сложных техник графического дизайна или использование продвинутых программ, таких как Photoshop. Для простых изменений, таких как замена года в сертификате с 2022 на 2023, необходимо только найти и скопировать цифру «3» в документе, после чего заменить имеющуюся «2». По аналогии, можно изменить и другие детали в документе. Например, замена имени или фамилии может быть осуществлена путем копирования букв из другого места документа.

Далее обычно все отсканированные

документы собираются либо в PDF либо в zip-архивы. Такие действия обычно приводят к скрытию (непреднамеренному или преднамеренному) специальных метаданных, содержащихся в фотографии, по которым можно было бы определить, что отсканированная копия документа содержала следы редактирования графических программ.

Один из наиболее простых способов определить использование графических программ в процессе обработки документа – это обратить внимание на цветовую гамму. Отсканированные документы обычно отображаются в градациях серого, с использованием 24-битных оттенков. Однако в попытке уменьшить объем занимаемого места или же с целью скрыть следы редактирования, многие часто прибегают к монохромному режиму и низкому разрешению сканирования (например, 150DPI на 150DPI). Подобные меры по оптимизации размеров отсканированных документов могут ощутимо сократить объемы данных на файловых серверах. Но, в то же время, это создает серьезные препятствия для последующего обнаружения подделок в сканах. Злоумышленники используют эту ситуацию в своих интересах, применяя различные техники, включая искажение углов документов, поднятие крышки сканера во время сканирования и т.д. Все эти действия осуществляются с целью ухудшения качества отсканированных копий и создания видимости случайных повреждений. В результате, отсканированные копии выглядят как «слегка и непреднамеренно испорченные», что затрудняет их анализ на предмет подделок.

Взаимодействие с экспертами-криминалистами, которые занимаются подготовкой судебных заключений, позволяет сделать вывод о том, что низкое качество сжатых сканов не обеспечивает достаточной информации для подтверждения изменений в отсканированных документах. Поэтому необходимо осознавать, что экономия на размере фотографий, особенно при снижении файла для хранения до 1 Мб не позволит достоверно установить факт подделки.

Следует отметить, что на оборудовании, используемом злоумышленником, и в помещениях, где происходил непосредственный физический контакт с компьютерной техникой могут быть также обнаружены и традиционные следы: следы пальцев рук; микрочастицы; следы обуви; записи систем видеонаблюдения; данные систем регистрации телефонных переговоров. Данные следы могут оставаться на поверхности компьютерной техники, периферийного оборудования и электронных цифровых носителей (клавиатура, мышь, магнитные носители, CD и DVD-диски, карты и др.).

Заключение.

1. Как показывает практика, процесс цифровизации жизнедеятельности общества, не мог не отразиться на таком негативном социальном явлении, как преступность. В настоящее время электронно-цифровые следы уже составляют значительную часть следов любого преступления, в связи с чем уяснение механизма их образования, источников их выявления, закрепления и приобщения к материалам расследования представляет практическую ценность сотрудников правоохранительных органов.

2. Склонны полагать, что при осуществлении следственных действий как в рамках расследования рассматриваемой разновидности преступлений, так и применительно к иным уголовным правонарушениям, помимо привлечения криминалиста, следует в обязательном порядке привлекать специалиста в области компьютерных технологий для выявления, фиксации и изъятия материальных объектов, на которых могут находиться электронно-цифровые следы. При выборе необходимого оборудования и определение наилучших технических методов для расследования каждой конкретной ситуации следует исходить из характера совершенного противоправного деяния.

Список использованной литературы:

1. Мещеряков, В.А. Основы методики расследования преступлений в сфере компьютерной информации: дис. … д-ра юрид. наук / В.А. Мещеряков. – Воронеж, 2001. – 387 с.
2. Борисов, В.В. Об особенностях фиксации информационных следов в практике защиты информации / В.В. Борисов // Известия Южного федерального университета. Технические науки. – 2009. – №5(94). – С. 164-168.
3. Шаповалова, Г.М. Возможность использования информационных следов в криминалистике (вопросы теории и практики): дис. … канд. юрид. наук. 12.00.09 / Г.М. Шаповалова. – Владивосток, 2005. – 198 с.
4. Касаткин, А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: автореф. дис. … канд. юрид. наук / А.В. Касаткин. – М., 1997. – 23 с.
5. Вехов, В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография / В.Б. Вехов. – Волгоград: ВА МВД России, 2008. – 404 с.
6. Милашев, В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ: автореф. дис. … канд. юрид. наук / В.А. Милашев. – М., 2004. – 18 с.
7. Россинская, Е.Р. Криминалистическое исследование компьютерных средств и систем как новый раздел криминалистической техники [Электронный ресурс]: материалы междунар. науч.-практ. конф.; отв. ред. А.А. Протасевич. – Байкальский государственный университет (Иркутск), 2014. – С. 317-325. – Режим доступа: https://elibrary.ru/download/elibrary_23791198_70740334.pdf (дата обращения: 27.05.2023).
8. Мещеряков, В.А. Виртуальные следы под «скальпелем Оккама» / В.А. Мещеряков // Информационная безопасность регионов. – 2009. – №1(4). – С. 28-33.
9. Shevchuk, V. Problems of formation and prospect for development of Criminalistic innovation; In: Zachar, Š., Meteňko, J., Meteňková, M. / Kriminalistika a forenzné vedy: veda, vzdelávanie, prax: 17. – Zborník príspevkov, 2021. – Pp. 323-338.
10. M. Madden, S. Fox, A. Smith and J. Vital. The nature of personal information is changing in the age of Web 2.0 / Pew Research Center, 2007 [Electronic resource] – Access mode: https://www.pewresearch.org/internet/2007/12/16/digital-footprints/ (Access data: 28.07.2023).
11. Цифровая криминалистика: учебник для вузов / В.Б. Вехов [и др.]; под ред. В.Б. Вехова, С.В. Зуева. – М.: Издательство Юрайт, 2021. – 417 с.
12. Смушкин, А.Б. Квопросу о наименовании теории «Электронная цифровая криминалистика» // Проблемы уголовного процесса, криминалистики и судебной экспертизы. – 2019. – №1(13). – С. 15-21.
13. Sammons, J. The basics of digital forensics / J. Sammons. – Amsterdam: Syngress Media, 2015. – 200 p.
14. Holt, T.J. Cybercrime and Digital Forensics: An Introduction (3rd ed.) / T.J. Holt, A.M. Bossler, K.C. Seigfried-Spellar. – Routledge, 2022. – 812 p.
15. Developments of criminalistics theory and future of forensic expertology: liber amicorum profesoriui Egidijui Vidmantui Kurapkai / Collective monography. – Vilnius, 2022. – 608 p.

References:

1. Meshherjakov, V.A. Osnovy metodiki rassledovanija prestuplenij v sfere komp'juternoj informacii: dis. … d-ra jurid. nauk / V.A. Meshherjakov. – Voronezh, 2001. – 387 s.
2. Borisov, V.V. Ob osobennostjah fiksacii informacionnyh sledov v praktike zashhity informacii / V.V. Borisov // Izvestija Juzhnogo federal'nogo universiteta. Tehnicheskie nauki. – 2009. – №5(94). – S. 164-168.
3. Shapovalova, G.M. Vozmozhnost' ispol'zovanija informacionnyh sledov v kriminalistike (voprosy

teorii i praktiki): dis. … kand. jurid. nauk. 12.00.09 / G.M. Shapovalova. – Vladivostok, 2005. – 198 s.

4. Kasatkin, A.V. Taktika sobiranija i ispol'zovanija komp'juternoj informacii pri rassledovanii prestuplenij: avtoref. dis. … kand. jurid. nauk / A.V. Kasatkin. – M., 1997. – 23 s.

5. Vehov, V.B. Osnovy kriminalisticheskogo uchenija ob issledovanii i ispol'zovanii komp'juternoj informacii i sredstv ejo obrabotki: monografija / V.B. Vehov. – Volgograd: VA MVD Rossii, 2008. – 404 s.

6. Milashev, V.A. Problemy taktiki poiska, fiksacii i iz#jatija sledov pri nepravomernom dostupe k komp'juternoj informacii v setjah JeVM: avtoref. dis. … kand. jurid. nauk / V.A. Milashev. – M., 2004. – 18 s.

7. Rossinskaja, E.R. Kriminalisticheskoe issledovanie komp'juternyh sredstv i sistem kak novyj razdel kriminalisticheskoj tehniki [Jelektronnyj resurs]: materialy mezhdunar. nauch.-prakt. konf.; otv. red. A.A. Protasevich. – Bajkal'skij gosudarstvennyj universitet (Irkutsk), 2014. – S. 317-325. – Rezhim dostupa: https://elibrary.ru/download/elibrary_23791198_70740334.pdf (data obrashhenija: 27.05.2023).

8. Meshherjakov, V.A. Virtual'nye sledy pod «skal'pelem Okkama» / V.A. Meshherjakov // Informacionnaja bezopasnost' regionov. – 2009. – №1(4). – S. 28-33.

9. Shevchuk, V. Problems of formation and prospect for development of Criminalistic innovation; In: Zachar, Š., Meteňko, J., Meteňková, M. / Kriminalistika a forenzné vedy: veda, vzdelávanie, prax: 17. – Zborník príspevkov, 2021. – Pp. 323-338.

10. M. Madden, S. Fox, A. Smith and J. Vital. The nature of personal information is changing in the age of Web 2.0 / Pew Research Center, 2007 [Electronic resource] – Access mode: https://www.pewresearch.org/internet/2007/12/16/digital-footprints/ (Access data: 28.07.2023).

11. Cifrovaja kriminalistika: uchebnik dlja vuzov / V.B. Vehov [i dr.]; pod red. V.B. Vehova, S.V. Zueva. – M.: Izdatel'stvo Jurajt, 2021. – 417 s.

12. Smushkin, A.B. K voprosu o naimenovanii teorii «Jelektronnaja cifrovaja kriminalistika» // Problemy ugolovnogo processa, kriminalistiki i sudebnoj jekspertizy. – 2019. – №1(13). – S. 15-21.

13. Sammons, J. The basics of digital forensics / J. Sammons. – Amsterdam: Syngress Media, 2015. – 200 p.

14. Holt, T.J. Cybercrime and Digital Forensics: An Introduction (3rd ed.) / T.J. Holt, A.M. Bossler, K.C. Seigfried-Spellar. – Routledge, 2022. – 812 p.

15. Developments of criminalistics theory and future of forensic expertology: liber amicorum profesoriui Egidijui Vidmantui Kurapkai / Collective monography. – Vilnius, 2022. – 608 p.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Денис Викторович Воеводкин – Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының докторанты, құқықтану магистрі, e-mail: voevodkin.denis@gmail.com.

Воеводкин Денис Викторович – докторант Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, магистр юриспруденции, e-mail: voevodkin.denis@gmail.com.

Voevodkin Denis Viktorovich – doctoral student of the Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Master of Jurisprudence, e-mail: voevodkin.denis@gmail.com.