Научная статья
УДК/UDC 343.9
DOI: 10.21779/2224-0241-2024-51-3-155-161

Цифровое алиби: понятие, сущность, проверка

А. В. Малык
Воронежский государственный университет, Воронеж, Российская Федерация, *nastena.malyk.95@mail.ru*

Аннотация: Актуальность исследования обуславливается фактическим увеличением количества ссылок подозреваемых и обвиняемых на «цифровое алиби». В настоящей статье рассматриваются основные аспекты «цифрового алиби»: понятие, его сущностное значение, а также перечень следственных действий, оперативно-розыскных мероприятий и тактических приёмов, необходимых при его установлении и проверке. Уделяется внимание необходимости выделения и адаптации одноимённых тактических операций. Предлагается рассмотреть виртуальные следы в качестве основы «цифрового алиби». Анализируется сложность выявления и фиксации виртуальных следов. В ходе работы поднимаются проблемы, недостаточности доказательственного значения «цифрового алиби» в Российской Федерации. Предлагается авторская трактовка понятия «цифрового алиби» в широком смысле. Обосновывается изменение направления основных следственных действий с учётом предложенного понятия «цифрового алиби».

Ключевые слова: цифровое алиби, виртуальные следы, цифровые информационные системы, тактические операции

Для цитирования: Малык А. В. Цифровое алиби: понятие, сущность, проверка // Юридический вестник ДГУ. 2024. Т. 51, № 3 (71). С. 155–161. DOI: 10.21779/2224-0241-2024-51-3-155-161

Original article

Digital alibi: concept, essence, verification

Anastasiya V. Malyk
Voronezh State University, Voronezh, Russian Federation, *nastena.malyk.95@mail.ru*

Abstract: The relevance of the study is determined by the actual increase in the number of references of suspects and defendants to "digital alibi". This article considers the main aspects of "digital alibi": the concept, its essential meaning, as well as the list of investigative actions, operative-search activities and tactical methods necessary in its establishment and verification. Attention is paid to the necessity of singling out and adapting tactical operations of the same name. It is proposed to consider virtual traces as the basis of "digital alibi". The complexity of identifying and fixing virtual traces is analysed. The work raises the problems of insufficient evidentiary value of "digital alibi" in the Russian Federation. The author's interpretation of the concept of "digital alibi" in a broad sense is offered. The change of the direction of the main investigative actions with the account of the proposed concept of "digital alibi" is substantiated.

Keywords: digital alibi, virtual traces, digital information systems, tactical operations

For citation: Malyk A. V. Digital alibi: concept, essence, verification. *Yuridicheskii vestnik DGU = Law Herald of DSU*, 2024, vol. 51, no. 3 (71), pp. 155–161. DOI: 10.21779/2224-0241-2024-51-3-155-161. (In Russ.).

Установление алиби подозреваемых и обвиняемых в ходе расследования преступлений является насущной необходимостью.

Согласно ч. 1 ст. 5 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ), алиби трактуется как: «нахождение подозреваемого или обвиняемого в момент совершения преступления в другом месте» [18, с. 431].

О. Я. Баев, ссылаясь на немецких криминалистов А. Форкера и В. Грайхэна, определяет алиби как: «доказанное отсутствие уголовно-релевантного лица (свидетеля, подозреваемого, обвиняемого) на уголовно-релевантном месте (место происшествия в широком смысле слова) во время происшествия или в иной удостоверенный объективно промежуток времени» [2, с. 385].

О. Н. Алексиенко даёт следующую трактовку понятия: «Алиби – это факт, влекущий отказ от уголовного преследования невиновного лица, которое в момент совершения преступления находилось в другом месте» [1, с. 8].

М. И. Николаева интерпретирует алиби как «подлежащий проверке довод либо факт, который установлен следствием или судом, свидетельствующий о нахождении подозреваемого или обвиняемого во время совершения преступления в ином месте, что может доказывать его невиновность» [12, с. 14].

А. Т. Тимербаев считает, что заявление об алиби – «это подлежащий проверке довод подозре-

ваемого или обвиняемого (подсудимого) о том, что данное лицо во время совершения преступления находилось в другом месте и поэтому оно не причастно к расследуемому преступлению» [14, с. 5].

Мы больше склоняемся к определению, сформулированному О. Я. Баевым, так как у других авторов фигурируют понятия «факт» и «довод», не совсем, на наш взгляд, подходящие для определения алиби.

Исходя из этимологии указанных слов, под фактом понимается событие или результат. Поскольку алиби – понятие юридическое, уместно рассмотреть понятие юридический факт. Под ним понимается – «предусмотренные нормой права обстоятельства, служащие основанием для возникновения (а также изменения или прекращения) конкретных правоотношений» [7].

Нахождение лица в определённом месте, например, в парке, даже впоследствии подтверждённое многочисленными свидетельскими показаниями, не всегда приводит к возникновению, изменению или прекращению правоотношений.

К тому же даже подтверждённое алиби лица, его заявляющего, не гарантирует отказ от уголовного преследования. Например, установлено, что лицо в определённый промежуток времени находилось на мероприятии в месте многочисленного скопления людей. Однако близость нахождения места совершения преступления не исключает, что он мог отлучиться и спокойно вернуться или побывать там после окончания мероприятия.

Согласно толковому словарю, под доводом понимается «мысль, соображение, приводимые в доказательство чего-нибудь, аргумент» [17]. Юридический довод толкуется как «имеющее юридическое основание высказывание субъекта юридической аргументации, сформулированное юридическим языком в виде суждения или умозаключения как формах правового мышления, несущее правовую информацию, сделанное для подтверждения обосновываемого им правового положения (тезиса) или для опровержения правового положения, обосновываемого другим соаргументатором» [7, с. 51].

Толкование понятия «довод», на наш взгляд, является более подходящим, чем понятие «факт». Однако наличие в определении М. И. Николаевой одновременно двух терминов делает его перегруженным, а отсутствие термина «довод» в законодательном определении алиби подводит нас к выводу, что оно также является не совсем уместным.

Итак, можно предположить, что понятие алиби, сформулированное О. Я. Баевым, более точное, поскольку законодатель трактует алиби как: «нахождение лица…» – это не что иное, как обстоятельство. Поскольку алиби рассматривается в рамках установления события преступления, не указано в закрытом перечне доказательств, но полежит установлению, оно представляет собой обстоятельство, подлежащее доказыванию. Именно это и указывается О. Я. Баевым – «доказанное отсутствие уголовно-релевантного лица» [2, с. 385], т.е. доказанное обстоятельство. Также данное определение не выходит за рамки общего понятия доказательств, что не противоречит УПК РФ, а широкий субъектный состав «отсутствие уголовно-релевантного лица (свидетеля, подозреваемого, обвиняемого)» [2, с. 385], указанного определения, раскрывает весь потенциал категории алиби.

Традиционно алиби устанавливается свидетельскими показаниями, подтверждающими местонахождение лица, в уголовно-релевантное время. При его проверке используются целый комплекс тактических приёмов [5, с. 11]: «эмоциональное воздействие, т.е. призыв к раскаянию и признанию вины, воздействие на лучшие стороны подозреваемого или обвиняемого с применением фактора внезапности; использование логического воздействия, т.е. предъявление доказательств, опровергающих показания, полученные в ходе допроса и требующих от обвиняемого детализации своих и чужих показаний, логический анализ противоречий, имеющихся в сведениях допрашиваемого» [15, с. 135].

Однако научно технический прогресс, обусловивший широкое распространение информационных технологий, предоставил возможность установления алиби с их помощью.

Обоснование нового вида алиби – «цифрового алиби» связанно с взаимодействием с различными цифровыми информационными системами: компьютерами, мобильными телефонами, системами видеонаблюдения и т.д.

Изначально «термин Digital alibi – цифровое алиби, появился в западных странах» [15, с. 134]. Под ним понимается: «факт непосредственного взаимодействия подозреваемого (обвиняемого) с компьютерным устройством, находящимся в другом месте в момент совершения преступления» [14, с. 437].

И.П. Понамарев трактует понятие «цифрового алиби» в широком и узком смыслах. В «широком» – как: «факт нахождения обвиняемого или подозреваемого вне места совершения преступления в момент, зафиксированный как время совершения преступления» [13, с. 270]. В «узком» смысле – как: «факт работы подозреваемого или обвиняемого с компьютером, находящимся вне места совершения преступления, в момент, зафиксированный как время преступления» [13, с. 270].

Определение в «узком» смысле, на наш взгляд, не содержит основных признаков «цифрового алиби» и, как выразилась Л.Б. Краснова, «скорее подразумевает вид, чем элемент общего понятия» [8, с. 105].

Полагаем, мнение Л.Б. Красновой оправдано, поскольку «цифровое алиби» включает не только работу за компьютерными устройствами, но и выход в «Интернет», текстовые, аудио и видео сообщения, определение местоположения устройства, записи камер видеонаблюдения, фиксацию видеорегистраторами, различные аудио-записи, и иные способы использования различных информационных систем, так или иначе подтверждающих нахождение лица в месте, отличном от совершения преступлений.

Как любая причина ведёт к определённому следствию, так и любое изменение обстановки находит своё отражение в действительности. Это значит, что взаимодействие лица с электронными системами приводит к образованию различных следов.

Научные работы В. И. Шиканова, Н. В. Кручининой, А. Т. Тимербаева и других авторов, посвящённые проблемам проверки и установления алиби, основаны на исследовании материальных и идеальных следов. Однако появление виртуальных следов, повлекшее за собой возникновение «цифрового алиби» изменило сущностное понимание содержания, принципов и приёмов ранее разработанных тактических операций «Проверка алиби» и «Предвосхищающая проверка алиби» [2, с. 385], сущность которых заключается в выявлении ложного алиби и предупреждении противодействия расследованию и раскрытию преступлений.

Необходимость адаптации тактических операций «Проверка алиби» и «Предвосхищающая проверка алиби» для установления «цифрового алиби» с каждым годом возрастает, поскольку инновационные технологии постоянно развиваются и, соответственно, становятся негласными свидетелями наших «беззаконий» или, наоборот, «добропорядочного поведения».

Проверка «цифрового алиби», как и «классического», подчиняется принципам, разработанным в криминалистической литературе, хотя и имеет определенную специфику. Такая специфика выражается в следовой картине «цифрового алиби».

Поскольку цель установления алиби, заключается в выяснении местоположения лица, в отношении которого имеются основания полагать о его причастности, и значимым фактором является установленный промежуток времени, то обнаруженные следы, необходимо оценивать и с учётом временных параметров.

К материальным следам взаимодействия с цифровой информационной системой И.П. Понамарёв относит: «следы на периферийном оборудовании, клавишах, других материальных объектах, участвующих в процессе работы, распечатках остаются пальцев рук, следы табака и т.д., которые трудно привязать к определенному времени, особенно при постоянном контакте» [14, с. 439].

К идеальным следам взаимодействия с цифровой информационной системой относится мысленный образ воспринятого подозреваемым (обвиняемым). И. П. Понамарёв подчёркивает, что «идеальные следы содержат информацию о таких сторонах объекта, которые не отображаются в материальных следах и могут использоваться для установления как причинно-следственных и пространственно-временных связей. Однако их точность и достоверность относительна, поскольку зависит от психических процессов восприятия информации конкретного лица, исключая её заведомое искажение» [14, с. 439].

«Данная классификация, как мы указывали в других работах, считается устоявшейся, однако цифровой век обусловил возникновение следов, которые не могут быть в полной мере отнесены ни к одной из вышеперечисленных групп, хотя обнаруживают в себе свойства обеих. Решающим критерием их выделения становится наличие однородных и специфических по своей природе научно обоснованных приемов и методов обнаружения, извлечения (фиксации), исследования и оценки следов. Такие следы было предложено назвать виртуальными следами» [10, с. 48].

В. А. Мещеряков определяет виртуальные следы как: «взаимосвязанный комплекс материально зафиксированной цифровой информации как результат специально организованного выборочного электронно-цифрового отражения фрагментов окружающей действительности в искусственной среде и знаний о формализованной модели, положенной в основу создания этой среды электронно-цифрового отражения» [11, с. 145]. Полагаем, что «дает возможность раскрыть часть материальной природы виртуального следа, так как это комплекс материально зафиксированной цифровой информации, и в то же время подводит нас к идеальным следам путём отсылки к параметрам абстрактной модели» [10, с. 49].

Природа виртуальных следов обусловлена пространственно-временными характеристиками, имеющими доказательственное значение для установления цифрового алиби. Итак, местом образования виртуальных следов является кибернетическое пространство. Под киберпространством понимается «среда, которая представляет собой следствие результата взаимодействия людей, программного обеспечения и услуг в Интернете с помощью технологий устройств и сетей, подключенных к ней, которых не существует в какой-либо физической форме» [9, с. 115].

Привязка виртуальных следов ко времени также обусловлена их природой. Поскольку киберпространство изначально подразумевает отсутствие существования следов в физической форме, то дополнительной характеристикой является время их формирования.

Указанные особенности виртуальных следов способствует установлению криминалистически значимой информации с помощью цифровых информационных систем.

Также одной из особенностей виртуальных следов, образующих доказательственную информацию, является их неустойчивость, выражающаяся в возможности легкой модификации, что увеличивает вероятность фальсификации, с целью создания ложного алиби.

Однако такая неустойчивость виртуальных следов восполняется многоаспектностью их разновидностей, в связи с чем фальсификация, обусловленная уничтожением, модификацией или изменением виртуальных следов взаимодействия с компьютерными системами, порождает другие следы, свидетельствующие о малейшем инородном вмешательстве. Определение наличия, указанных из-

менений, возможно лишь при достаточном объеме специальных знаний о технических и временных характеристик соответствующих файлов.

Отсюда следует, что следовая картина «цифрового алиби» всегда представляет собой, наличие или отсутствие дополнительного вида следов, взаимодействия с цифровыми информационными системами – «виртуальных следов».

Таким образом, цифровое алиби включает:

1. «время совершения преступления,
2. место его совершения
3. место фактического нахождения заявителя алиби в момент совершения преступления» [14, с. 441];
4. следов – виртуальных.

Основным источником доказательств в цифровом алиби, в отличии от классического, являются цифровые информационные системы.

Исходя из вышесказанного, можно сделать вывод, что «цифровое алиби» представляет собой обстоятельство, подтверждающее деятельность субъекта, неразрывно связанную с намеренным или ненамеренным использованием многочисленных информационных систем, функционирующих на разных технологических основаниях, фиксирующих определённое изменение информации в уголовно релевантное время в месте, отличном от совершения преступления, посредством образования преимущественно виртуальных следов.

На основании предложенного нами определения установление «цифрового алиби» требует подтверждения следующих обстоятельств:

1. полного перечня цифровых информационных систем и устройств, с которыми лицо, заявившее о «цифровом алиби» осуществляло взаимодействие целенаправленно, либо ненамеренно (могло быть ими зафиксировано тем или иным способом) и данных о цифровых информационных системах и устройствах (по возможности – вид, марка, модель и т.д.);

2. территориального нахождения цифровых информационных систем в месте, отличном от совершения преступления;

3. факта непосредственного взаимодействия с цифровыми информационными системами и устройствами лица, в отношении которого осуществляется проверка.

Допрос при установлении «цифрового алиби» очень важен, однако он не должен ограничиваться односторонним направлением. Он должен учитывать всевозможные направления работы различных цифровых информационных систем, которые тем или иным образом могут являться источниками, содержащими информацию, имеющую значение для установления местонахождения лица.

Именно правильная формулировка вопросов, касающаяся специфического характера функционирования цифровых информационных систем, проработанная следователем совместно с участием специалиста, обеспечивает не только получение подробной информации от допрашиваемого лица, необходимое для проверки его слов, но и даёт возможность установления дополнительной информации из иных цифровых информационных систем, которая может стать независимым источником подтверждения или опровержения цифрового алиби, а также исключить намеренное создание ложного алиби» [4, с. 73].

При подготовке к допросу с целью проверки и установления цифрового алиби необходимо выяснить:

1. С какими конкретными цифровыми информационными системами и устройствами лицо непосредственно соприкасалось в интересующее время и дату.

2. Какие цифровые информационные системы и устройства могли зафиксировать его присутствие вне зависимости от действий лица, например, в силу своего стационарного нахождения;

3. Характер взаимодействия с указанными цифровыми информационными системами и устройствами.

4. Имели ли указанные цифровые информационные системы и устройства доступ к сети «Интернет», осуществлялся ли выход в «Интернет» при непосредственном взаимодействии.

5. При осуществлении выхода в «Интернет» осуществлялось ли взаимодействие с мессенджерами т. д. (данные об этих контактах).

6. Уровень профессиональных навыков и опыта работы допрашиваемого с цифровыми информационными системами.

Указанный перечень вопросов автоматически расширяет область поиска цифровой информации, тем самым увеличивая круг следственных и иных действий по установлению и проверке цифрового алиби.

Расширение области поиска цифровой информации подразумевает проверку «цифрового алиби», зафиксированного как стационарными цифровыми информационными системами, так и портативными цифровыми устройствами мобильными телефонами, смартфонами, ноутбуками, имеющими возможность выхода в сеть «Интернет».

Таким образом, меняется направление и характер следственных и иных действий по установлению «цифрового алиби». Добавляется активный поиск дополнительной информации, начинающийся с направления многочисленных запросов относительно фиксации, интересующей информации, различными цифровыми информационными системами.

Полагаем, что предложенное нами определение увеличивает круг источников цифрового алиби и делает его более доступным для понимания. Например, лицо заявляет, что находилось в интересующее время в определённом месте и наверняка могло попасть на камеры видеонаблюдения, записи с камер не дают сто процентной гарантии и не исключают возможности фальсификации, однако при производстве определённых процессуальных действий являются подтверждением нахождения лица в месте, где эти камеры установлены.

Установление алиби подразумевает использование таких тактических операций, как «Проверка алиби» и «Предвосхищающая проверка алиби», однако развитие научно-технического прогресса обусловило их изменение.

Адаптация, указанных тактических операций, должна осуществляться с учётом особенностей следовой картины виртуальных следов.

Таким образом, предложенное понимание цифрового алиби обуславливает необходимость использования «тактической операции проверка цифрового алиби» [3, с. 69], которая на основании вышесказанного не ограничиваются наличием специальных знаний и проведением компьютерных экспертиз, а представляет собой «комплекс оперативно-розыскных мероприятий, следственных и иных действий, направленный на поиск дополнительной информации о местонахождении лица в уголовно-релевантный промежуток времени, включающий: допросы, различные виды осмотра цифровых информационных систем и компьютерных устройств, установление соединений между абонентами» [18, с. 69], выемки электронных носителей, опросы, сборы образцов для сравнительного исследования, установление геопозиции портативных устройств путём подключения к навигационным сетям через спутниковые системы, установление территориального нахождения устройств, с которых осуществлялся выход в информационно-коммуникационную сеть «Интернет» и т.д.

Тактическая операция «проверка цифрового алиби» направлена на поиск и обнаружение виртуальных следов, и соответственно доказательств, сформированных на их основе, которые могут быть утрачены или сфальсифицированы, и при этом не иметь внешних признаков изменений, в силу особенностей цифровых информационных систем, чем собственно и осложняется деятельность по проверке и установлению «цифрового алиби».

«Предвосхищающая проверка цифрового алиби» преследует те же цели и осуществляется схожими способами, однако производится на первоначальном этапе расследования, до момента заявления цифрового алиби подозреваемым (обвиняемым), и представляет собой инициативный процесс поиска интересующей информации.

Указанные криминалистические тактические операции способствуют получению необходимой для выдвижения и проверки следственных версий информации.

Анализ полученной информации позволяет выдвинуть различные версии:

«подозреваемый (обвиняемый) имеет цифровое алиби;

подозреваемый (обвиняемый) цифрового алиби не имеет;

цифровое алиби подозреваемого (обвиняемого) сфальсифицировано» [14, с. 438].

«Цифровое алиби» становится весьма распространённой уголовно-релевантной и криминалистической категорией.

В уголовном процессе алиби представляет собой средство защиты. Криминалистическое значение алиби заключается в возможности построения новых следственных версий, которые определяет соответствующее направление расследования, изменяют его содержание, последовательность следственных действий, постановку новых задач и планирование расследования в целом.

Цифровая доказательственная информация крайне неустойчива. Это серьёзно усложняет процесс проверки и установления «цифрового алиби». Объективное установление заявленного «цифрового алиби» возможно только при осуществлении комплексного подхода, который обеспечивает доскональную и тщательную проверку субъектами расследования с целью формирования объективного вывода о ложности или истинности алиби подозреваемого.

Сложно не согласится с О. П. Виноградовой, которая считает, что «осуществление проверки «цифрового алиби» должно реализовываться с помощью использования криминалистической тактической операции «проверка цифрового алиби», которая должны включать, помимо стандартных приемов, действия, направленные на осмотр компьютера, иных электронных «гаджетов», установление соединений между абонентами, запросов по биллингу в телекоммуникационные компании, проведение компьютерных экспертиз и др.» [3, с. 69].

Полагаем, «предвосхищающая проверка цифрового алиби», также как и непосредственная, «должна представлять собой чёткий комплекс следственных действий, представляющий собой многоаспектную деятельность следователей, опероуполномоченных сотрудников, экспертов и специалистов, регламентированную рамками соответствующих тактических операций» [15], на основании разработанных следственных ситуаций, предполагающих выдвижение версий о «цифровом алиби», для существенной оптимизации следственного поиска.

Подводя итоги, можно сказать, что предложенное нами определение цифрового алиби, связанное с использованием широкого круга возможностей различных цифровых информационных систем, обеспечивает стабилизацию положения «цифрового алиби» как правовой категории, способствует усилению его доказательственного значения и увеличению ссылок подозреваемых и обвиняемых на цифровые источники информации, в подтверждение своей непричастности.

Список источников

1. *Алексиенко О. Н.* Криминалистические методы разоблачения ложного алиби по делам о преступлениях против жизни и здоровья: автореф. дис. … канд. юрид. наук. Ростов-на-Дону, 2009. 23 с.

2. *Баев О. Я.* Следователь (основы теории и практики деятельности) / О. Я. Баев. М.: «Прометей», 2017. 485 с.

3. *Виноградова О. П.* Криминалистические особенности исследования «цифрового алиби» // Известия ТулГУ. Экономические и юридические науки. 2023. №2. С. 64–70.

4. *Джабраилов И.И.* «Цифровое» алиби // Наука и техника. Мировые исследования: материалы XIV международной научно-практической конференции. Саратов, 2021. С. 70–74.

5. *Елфимов П.В., Виноградова О.П.* Ложное алиби как элемент механизма противодействия расследованию преступлений // Известия Тульского государственного университета. Экономические и юридические науки. 2022. № 3. С. 10–19.

6. *Елфимов П.В., Виноградова О.П.* Противодействие расследованию преступлений, связанных с нарушением авторских и смежных прав: проблемы тактики производства отдельных следственных действий // Вестник Могилевского института МВД. 2022. № 1(5). С. 44–48.

7. *Каргин К.В.* Юридический довод // Государство и право. 2020. № 6. С. 43–53.

8. *Краснова, Л. Б.* Использование особенностей информационных технологий для установления и проверки алиби / Л. Б. Краснова // Воронежские криминалистические чтения. 2014. № 16. С. 104–111.

9. *Малык А. В.* Особенности обеспечения доказательств: нотариальный осмотр информации в сети «Интернет» // Государство и право в цифровую эпоху : материалы международной научно-практической конференции Санкт-Петербург, 27 апреля 2022 г., Санкт-Петербург, 27 апреля 2022 года / Е. В. Трофимов. Санкт-Петербург: Санкт-Петербургский институт (филиал) ВГУЮ (РПА Минюста России), 2022. С. 114–121.

10. *Малык А. В.* Формирование и природа электронных доказательств // Вестник Воронежского государственного университета. Серия: Право. 2023. № 3(54). С. 45–51.

11. *Мещеряков В. А.* Теоретические основы механизма следообразования в цифровой криминалистике. М.: Проспект, 2022. 176 с.

12. *Николаева М. И.* Алиби: уголовно-процессуальный и криминалистический аспекты: автореф. дис. … канд. юрид. наук. М., 2005. 26 с.

13. *Пономарев И.П.* Цифровое алиби // Воронежские криминалистические чтения: сборник научных трудов. Воронеж: Изд-во Воронежского государственного университета, 2010. Вып. 12. С. 269–279.

14. *Пономарев И. П.* Цифровое алиби и его проверка // Вестник Воронежского государственного университета. Серия: право. 2011. № 3. С. 437–444.

15. *Романова А.В., Кулько В.В.* Проблемы проверки «цифрового алиби» // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2017. № 1. С. 134–139.

16. *Тимербаев А. Т., Сердюк Л. В.* Тактика проверки заявления об алиби на предварительном следствии: учебное пособие. Хабаровск: Хабаровская высшая школа МВД СССР, 1987. 62 с.

17. Толковый словарь русского языка: т. 1-4 / сост. Г. О. Винокур, проф. Б. А. Ларин, С. И. Ожегов [и др.] ; под ред. проф. Д. Н. Ушакова. Москва : Гос. ин-т «Советская энциклопедия», 1935-1940. Т. 1: А - Кюрины. Т. 1. 1935. LXXVI, 1562 стб.

18. *Туркина Д. А., Сафронова Е. В.* К вопросу о цифровом алиби в криминалистике // Технологии XXI века в юриспруденции: материалы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 430–438.

References

1. Aleksiyenko O. N. Kriminalisticheskiye metody razoblacheniya lozhnogo alibi po delam o prestupleniyakh protiv zhizni i zdorovya [Criminalistic methods of exposing false alibi in cases of offences against life and health]: Cand. Law sci. dis. abstr. Rostov-na-Donu, 2009. 23 p. (In Russ.).

2. Bayev O. YA. Sledovatel (osnovy teorii i praktiki deyatelnosti) [Investigator (basics of theory and practice of activity)]. Moscow, Prometey Publ., 2017, 485 p. (In Russ.).

3. Vinogradova O. P. Kriminalisticheskiye osobennosti issledovaniya "tsifrovogo alibi" [Criminalistic features of the study of "digital alibi"], *Izvestiya TulGU. Ekonomicheskiye i yuridicheskiye nauki [Izvestia TulSU. Economic and legal sciences]*, 2023, no. 2, pp. 64–70. (In Russ.).

4. Dzhabrailov I.I. "TSifrovoye" alibi ["Digital" alibi], *Nauka i tekhnika. Mirovyye issledovaniya [Science and Technology. World Studies]*: proceedings of the XIV International Scientific and Practical Conference. Saratov, 2021, pp. 70-74. (In Russ.).

5. YElfimov P.V., Vinogradova O.P. Lozhnoye alibi kak element mekhanizma protivodeystviya rassledovaniyu prestupleniy [False alibi as an element of the mechanism of counteraction to the investigation of crimes], *Izvestiya Tulskogo gosudarstvennogo universiteta. Ekonomicheskiye i yuridicheskiye nauki [Proceedings of Tula State University. Economic and legal sciences]*, 2022, no. 3, pp. 10-19. (In Russ.).

6. YElfimov P.V., Vinogradova O.P. Protivodeystviye rassledovaniyu prestupleniy, svyazannykh s narusheniyem avtorskikh i smezhnykh prav: problemy taktiki proizvodstva otdelnykh sledstvennykh deystviy [Countering the investigation of crimes related to the infringement of copyright and related rights: problems of

tactics of production of individual investigative actions], *Vestnik Mogilevskogo instituta MVD [Bulletin of the Mogilev Institute of the Ministry of Internal Affairs]*, 2022, no. 1(5), pp. 44-48. (In Russ.).

7. Kargin K.V. YUridicheskiy dovod [Legal argument], *Gosudarstvo i pravo [State and Law]*, 2020, no. 6, pp. 43-53. (In Russ.).

8. Krasnova L. B. Ispolzovaniye osobennostey informatsionnykh tekhnologiy dlya ustanovleniya i proverki alibi [Using the features of information technologies to establish and verify alibi], *Voronezhskiye kriminalisticheskiye chteniya [Voronezh forensic readings]*, 2014, no. 16, pp. 104-111. (In Russ.).

9. Malyk A. V. Osobennosti obespecheniya dokazatelstv: notarialnyy osmotr informatsii v seti "Internet" [Features of securing evidence: notarial inspection of information on the Internet], *Gosudarstvo i pravo v tsifrovuyu epokhu [State and law in the digital age]*: materials of the international scientific and practical conference St. Petersburg, April 27, 2022; E. V. Trofimov. Sankt-Peterburg: Sankt-Peterburgskiy institut (filial) VGUYU (RPA Minyusta Rossii) Publ., 2022, pp. 114-121. (In Russ.).

10. Malyk A. V. Formirovaniye i priroda elektronnykh dokazatelstv [Formation and nature of electronic evidence], *Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Pravo [Bulletin of the Voronezh State University. Series: Law]*, 2023, no. 3(54), pp. 45-51. (In Russ.).

11. Meshcheryakov V. A. Teoreticheskiye osnovy mekhanizma sledoobrazovaniya v tsifrovoy kriminalistike [Theoretical foundations of the mechanism of trace formation in digital forensics]. Moscow: Prospekt Publ., 2022, 176 p. (In Russ.).

12. Nikolayeva M. I. Alibi: ugolovno-protsessualnyy i kriminalisticheskiy aspekty [Alibi: criminal-procedural and criminalistic aspects]: Cand. Law sci. dis. abstr. Moscow, 2005, 26 p. (In Russ.).

13. Ponomarev I.P. TSifrovoye alibi [Digital alibi], *Voronezhskiye kriminalisticheskiye chteniya [Voronezh forensic readings]*: collection of scientific papers. Voronezh: Publishing House of Voronezh State University, 2010, issue 12, pp. 269–279. (In Russ.).

14. Ponomarev I. P. TSifrovoye alibi i yego proverka [Digital alibi and its verification], *Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: pravo [Bulletin of the Voronezh State University. Series: Law]*, 2011, no. 3, pp. 437–444. (In Russ.).

15. Romanova A.V., Kulko V.V. Problemy proverki "tsifrovogo alibi" [Problems of verification of "digital alibi"], *Prestupnost v sfere informatsionnykh i telekommunikatsionnykh tekhnologiy: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestupleniy [Crime in the field of information and telecommunication technologies: problems of prevention, disclosure and investigation of crimes]*, 2017, no. 1, pp. 134-139. (In Russ.).

16. Timerbayev A. T., Serdyuk L. V. Taktika proverki zayavleniya ob alibi na predvaritelnom sledstvii [Tactics of checking the alibi statement on the preliminary investigation]: a textbook. KHabarovsk: KHabarovskaya vysshaya shkola MVD SSSR Publ., 1987, 62 p. (In Russ.).

17. Tolkovyy slovar russkogo yazyka [Explanatory dictionary of the Russian language] : vol. 1-4 / the compiler G. O. Vinokur, prof. B. A. Larin, S. I. Ozhegov [and others] ; ed. by prof. D. N. Ushakov. Moscow: Gos. in-t "Sovetskaya entsiklopediya" Publ., 1935-1940. Vol. 1: A - Kyuriny. Vol. 1, 1935, LXXVI, 1562 p. (In Russ.).

18. Turkina D. A., Safronova YE. V. K voprosu o tsifrovom alibi v kriminalistike [To the question of digital alibi in criminalistics], *Tekhnologii XXI veka v yurisprudentsii [Technologies of the XXI century in jurisprudence]*: materials of the Fifth International scientific and practical conference. (Yekaterinburg, May 19, 2023), ed. by D. V. Bakhteev. YEkaterinburg: ANO "KrimLib" Publ., 2023, pp. 430–438. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Малык Анастасия Владимировна, аспирант кафедры криминалистики юридического факультета ФГБОУ ВО «Воронежский государственный университет», г. Воронеж, Российская Федерация. *E-mail: nastena.malyk.95@mail.ru*

Поступила в редакцию 25.04.2024 г.; одобрена после рецензирования 10.09.2024 г.; принята к публикации 12.09.2024 г.

INFORMATION ABOUT THE AUTHOR

Malyk Anastasiya Vladimirovna, Postgraduate student of the Department of Criminalistics, Faculty of Law, Voronezh State University, Voronezh, Russian Federation. E-mail: *nastena.malyk.95@mail.ru*

Received 25.04.2024; approved after reviewing 10.09.2024; accepted for publication 12.09.2024