Научная статья
УДК 342.9: 343.985

ЦИФРОВОЙ ПРОФИЛЬ ФИЗИЧЕСКОГО ЛИЦА КАК НОВЫЙ БАЗИС КРИМИНАЛИСТИЧЕСКОЙ РЕГИСТРАЦИИ

Борис Валерьевич Асаёнок
Международный университет «МИТСО», Минск, Республика Беларусь,
boris.asayonok@gmail.com, https://orcid.org/0000-0001-8410-682X

Аннотация. В данной научной статье изложены авторские подходы к рассмотрению цифрового профиля и цифрового следа как правовых категорий применительно к криминалистическим аспектам доказывания в уголовном и административном процессах. Эти правовые категории являются достаточно известными в правовой сфере, но до сих пор нет четкой доктринальной точки зрения на их место в категориальном аппарате и системе криминалистической регистрации. Излагается позиция о возможности использования цифрового профиля в качестве стержневого элемента построения современной системы криминалистических учетов, предлагаются рекомендации о некоторых подходах построения криминалистических учетов на данных принципах.

Ключевые слова: киберкриминалистика, цифровой след, цифровой профиль, теория доказывания.

Для цитирования: Асаёнок Б. В. Цифровой профиль физического лица как новый базис криминалистической регистрации // Вестник Уфимского юридического института МВД России. 2024. № 3 (105). С. 95–103.

Original article

DIGITAL PROFILE OF AN INDIVIDUAL AS A NEW BASIS FOR FORENSIC REGISTRATION

Boris V. Asayonok
International University «MITSO», Minsk, Republic of Belarus
boris.asayonok@gmail.com, https://orcid.org/0000-0001-8410-682X

Abstract. This scientific article outlines the author's approaches to considering the digital profile and digital trace as legal categories in relation to forensic aspects of evidence in criminal and administrative proceedings. These legal categories are quite well known in the legal field, but there is still no clear doctrinal point of view on their place in the categorical apparatus and the system of forensic registration. The position on the possibility of using a digital profile as a core element in building a modern system of forensic records is outlined, and recommendations are offered on some approaches to building forensic records on these principles.

Keywords: cybercriminalistics, digital trace, digital profile, theory of evidence.

For citation: Asayonok B. V. Digital profile of an individual as a new basis for forensic registration // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2024. No. 3 (105). P. 95–103. (In Russ.)

Введение

Противоправная деятельность как негативная часть социальной активности человека в значительной мере прошла цифровую трансформацию. Большое количество правонарушений (влекущих административную и уголовную ответственность) совершается именно в цифровом пространстве. Этот фактор повышает уровень взаимодействия преступных сообществ различных стран,

затрудняя возможности привлечения виновных лиц к ответственности. Это, в свою очередь, негативно влияет на эффективность функционирования всех государственных и общественных институтов, охрану прав, свобод и законных интересов граждан.

Не вызывает сомнения тот факт, что количество киберпреступлений будет расти в обозримой перспективе. Российские источники указывают:

– за 2022 год количество преступлений в сети Интернет – 522 тысячи[1].

– за 2023 год количество преступлений в сети Интернет – 667 тысяч (на 30 % больше, чем в 2022 г.)[2].

Имеется общее увеличение преступлений, совершаемых в сети Интернет (при некотором снижении преступности с использованием компьютерных и программных средств), что указывает на изменение способов преступлений.

В Республике Беларусь хищения имущества путем модификации компьютерной информации в течение нескольких лет имеют следующую тенденцию: 2021 год – 1185, 2022 год – 1192, 2023 год – 1079[3]. Как видим, есть небольшая тенденция к снижению, но это всего лишь один год и по одному из видов киберпреступлений[4]. В целом же уголовное законодательство Республики Беларусь в рамках гл. 31 «Преступления против компьютерной безопасности» содержит пять видов киберпреступлений[5].

Не следует в данном направлении исключать борьбу с административными правонарушениями в киберпространстве, тем более, что некоторые из них (к примеру, предусмотренные ст. 23.4 «Несанкционированный доступ к компьютерной информации», ст. 23.7 «Нарушение законодательства о защите персональных данных» Кодекса Республики Беларусь об административных правонарушениях) весьма схожи с преступлениями и на начальном этапе выявления и пресечения не всегда бывает возможным установить к какой сфере законодательства данное правонарушение относится[6]. Аналогичный подход к установлению административной ответственности имеет место и в Российской Федерации, о чем свидетельствуют отдельные научные работы [1].

В контексте борьбы с киберпреступностью уже несколько десятков лет развивается такое направление криминалистической науки, как киберкриминалистика (цифровая криминалистика, форензика и другие названия – суть одной и той же концепции научного знания), в рамках которой проводятся исследования различными учеными-криминалистами (к примеру, О. И. Лозинским [2], А. А. Троицким [3], Н. Н. Федотовым [4] и др.). Однако формирование данного направления не отменяет традиционной системы криминалистики, которая позволяет систематизировать и структурировать новые знания, полученные в ходе раскрытия и расследования преступлений в цифровом пространстве. Отдельные классические отрасли криминалистической техники

---

[1] МВД: число преступлений с использованием IT-технологий выросло на 23,5 % // Ведомости 25. URL: https://www.vedomosti.ru/society/news/2024/04/08/1030570-chislo-prestuplenii-s-ispolzovaniem-it-tehnologii-viroslo (дата обращения: 20.06.2024).

[2] Ущерб от киберпреступлений в России за пять лет оценили в 500 млрд рублей // Информационная группа «Интерфакс». URL: https://www.interfax.ru/russia/962511 (дата обращения: 20.06.2024).

[3] Верховный Суд Республики Беларусь. https://court.gov.by/ru/justice_rb/statistics/69694c4d3e774d6e.html (дата обращения: 22.03.2024).

[4] К сожалению, нам не удалось обнаружить в открытом доступе информацию по всем видам киберпреступлений (а также информацию именно по зарегистрированным преступлениям), в силу чего статистические данные представлены в несколько ограниченном виде.

[5] Уголовный кодекс Республики Беларусь // ООО «ЮрСпектр». Нац. центр правовой информ. Респ. Беларусь. Минск, 2024 (дата обращения: 20.06.2024).

[6] Кодекс Республики Беларусь об административных правонарушениях // ООО «ЮрСпектр». Нац. центр правовой информ. Респ. Беларусь. Минск, 2024 (дата обращения: 20.06.2024).

и тактики становятся основой для работы в цифровой реальности. Криминалистическое учение о следах позволяет развить категорию «цифровой след», в русле организации и тактики отдельных следственных или процессуальных действий формируются криминалистические рекомендации по работе с цифровыми доказательствами. Организация и тактика назначения и проведения экспертизы позволяет в полной мере систематизировать вопросы извлечения криминалистически значимой информации из цифровых следов и их носителей.

Практика, обогащенная техническими и программными методами познания цифровой реальности, показывает определенные результаты, но они должны опираться на практическое изучение постоянно изменяющейся сферы преступного применения киберпространства. Теория же, к сожалению, опирается во многом на категориальный аппарат конца XX – начала XXI века и не выработала единых подходов к тому, как обобщать, систематизировать опыт борьбы с киберпреступностью.

Пребывание в цифровом пространстве так же, как и в материальном мире оставляет многочисленные следы, в том числе и имеющие значение для раскрытия, расследования и предупреждения различных правонарушений. Представляется важным постоянно систематизировать их изучение не только в контексте криминалистической регистрации. Традиционно криминалистические учеты представляются системой сосредоточения, хранения и пользования криминалистически значимой информацией, где цифровая форма информации рассматривается лишь в качестве одной из форм учета криминалистически значимых признаков (наряду с письменной/печатной, коллекционной). Однако признание за цифровой реальностью и цифровыми следами самостоятельного значения в качестве криминалистически значимых категорий требует новых подходов к системе организации криминалистических и оперативных учетов.

Речь идет прежде всего о криминалистическом профилировании физического лица. Имеет значение криминалистическое профилирование также для выявления, пресечения административных правонарушений. С учетом этого профилированию могут подвергаться и юридические лица. К примеру, это имеет значение при изучении субъектов экономической деятельности, при выявлении и пресечении таможенных и налоговых правонарушений. Значимо такое профилирование и для предупреждения и пресечения административных правонарушений в рамках административно-юрисдикционной деятельности государственных органов (таможенный, пограничный, санитарно-ветеринарный и другой контроль). Все это позволяет вывести на новый практический уровень категорию цифрового криминалистического профиля.

Методы

Данная проблематика является самостоятельным аспектом ряда частных криминалистических теорий, интегрирующих их на базе необходимости разработки нового поискового инструментария. Основой этого исследования стал диалектический материализм, позволяющий изучать динамику криминалистически значимых явлений. Взаимосвязи структурных составляющих цифрового профиля исследовались с учетом системно-деятельностного подхода. Основными специальными юридическими методами стали: сравнительно-правовой и метод криминалистической систематики.

Результаты

Криминалистический профиль как категория имеет распространение в отечественной (постсоветской) криминалистике. Если изначально это было некое подражание зарубежному опыту (например, попытки составления психологического профиля преступника по делам о тяжких насильственных преступлениях), то в настоящее время это абсолютно самодостаточная отечественная криминалистическая категория. Е. С. Черкасова в этой связи считает тождественными психолого-криминалистический профиль (портрет) преступника и криминалистическую характеристику преступника [5, с. 133]. Е. И. Фойгель еще

ранее в контексте поиска преступника дала следующее определение поисково-криминалистическому профилю – «совокупность криминалистически значимых признаков лица, совершившего преступление, сформированных в результате анализа обстановки преступления в целях розыска и установления неизвестного преступника» [6, с. 55]. М. А. Аперонова, обобщая ранее предложенные криминалистической доктриной характеристики данного термина, предложила свое комплексное понятие – криминалистическая характеристика профиля гражданина примерно с тем же содержанием, что и указанные ранее категории [7, с. 459].

Профиль физического лица не является чем-то новым для правовой реальности. Так, к примеру, постановление Правительства Российской Федерации от 3 июня 2019 г. № 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» оперирует данным термином и регламентирует отдельные сценарии использования цифрового профиля в открытом цифровом пространстве. В соответствии с данным нормативным правовым актом: «цифровой профиль – это совокупность цифровых записей о гражданине, содержащихся в информационных системах государственных органов и организаций. Инфраструктура цифрового профиля построена на основе единой системы идентификации и аутентификации (ЕСИА)»[1]. При его использовании компетентные субъекты получают возможность к доступу информационных баз государственных органов, содержащих информацию о физических лицах, вступавших во взаимодействие с ними. Таким образом, цифровой профиль представляет собой систематизированные посредством поискового запроса данные о физическом лице в процессе его взаимодействия с государственным органами, учреждениями и организациями. К сожалению, белорусское законодательство еще не имеет в широком употреблении определения цифрового профиля, хотя попытки ввести его в правовое поле имеются. Так, проект Государственного стандарта Республики Беларусь «Цифровая трансформация. Термины и определения» дает определение схожей категории: цифровой образ – «совокупность характеристик субъекта или объекта реального мира, сущности в цифровой форме, однозначно характеризующая субъект или объект и его состояние» [8, с. 258]. Здесь же дается и определение цифрового пространства в качестве пространства, интегрирующего цифровые процессы, средства цифрового взаимодействия, информационные ресурсы, а также совокупность цифровых инфраструктур на основе норм регулирования, механизмов организации, управления и использования [8, с. 258].

Такой недостаток правовой регламентации на национальном уровне вместе с тем не препятствует возможностям раскрыть его содержание с позиций криминалистической, оперативно-розыскной и административно-правовой доктрин[2]. Возможности открытого доступа к информации о физическом лице чрезвычайно широки в сети Интернет. В особенности это касается социальных сетей, а также иных сфер, где физическое лицо самостоятельно сообщает информацию о себе либо дает согласие на распространение такой информации.

Сам цифровой профиль, по мнению отдельных исследователей, содержит группы

---

[1] Сценарии использования инфраструктуры Цифрового профиля. URL: https://digital.gov.ru/uploaded/presentations/stsenarii-ispolzovaniya-infrastrukturyi-tsp-13_w6nhiEs.pdf?utm_referrer=https%3a%2f%2fwww.google.com%2f (дата обращения: 04.03.2024).

[2] Мы считаем необходимым говорить о возможности выявления и преступлений, и административных правонарушений криминалистическими и оперативно-розыскными методами, поскольку на момент выявления правонарушения не всегда возможно дать его квалификацию. Кроме того, в криминалистической доктрине достаточно развито учение о криминалистическом обеспечении производства по делам об административных правонарушениях.

идентификаторов: традиционные идентификаторы для физического лица в виде его персональных данных; сведения в государственных электронных информационных базах; биометрические данные; информационно-технологические идентификаторы, используемые в цифровых устройствах и сервисах, компьютерных системах, информационно-телекоммуникационной сети Интернет, сетях связи, банковской и платежной системах [9, с. 305]. В некоторых случаях высказывается даже мнение о возможности в рамках цифрового профиля осуществлять автоматическую идентификацию следов посредством внедрения соответствующих алгоритмов [10, с. 104].

Однако, как видится, роль цифрового профиля может быть более значимой. Он может явиться базовой криминалистической категорией и технологией для трансформации всей системы криминалистических учетов, в том числе на основе использования искусственного интеллекта. Объем данных о физическом лице в цифровой форме будет только расти. Если в основу построения криминалистических учетов вновь ввести принцип построения не от криминалистически значимого признака к человеку, а от человека к признаку, то имеющаяся в открытом доступе цифровая информация становится базисом для всей системы криминалистических учетов. Далее к ним присоединяется информация из профилей лица в системах цифрового общения с государственными органами и системами, профили лица в социальных сетях, электронная переписка и т. п. Оцифровке могут быть подвергнуты (или уже подвергнуты) данные медицинского характера, персональная биологическая информация, не говоря уже о всей системе криминалистически значимых признаков (дактокарты в электронном виде, снимки радужной оболочки глаз, цифровые снимки внешности и т. п.).

Однако собирать такую информацию в режиме запроса-ответа каждый раз, когда такая информация требуется, неэффективно. Если дать алгоритму искусственного интеллекта действовать в режиме постоянного накопления цифровой информации о лице, уже однажды попавшем в сферу внимания правоохранительных органов, то это позволяет формировать динамическое цифровое досье (цифровой криминалистический профиль). Такое цифровое досье – цифровой криминалистической профиль – будет на конкретную единицу времени содержать все необходимые данные, позволяющие установить обстоятельства, связывающие его с противоправным деянием.

Одновременно с этим следует совершенствовать такое направление, как использование цифрового профиля для идентификации лица. По мнению Ю. Д. Уздяевой, «криминалистическое значение профиля состоит в реализации таких функций, как идентификация без необходимости предоставления бумажных документов»[1]. Постановка данного вопроса как направления выявления и пресечения противоправных деяний не только правомерна, но уже в полной мере реальна для правоохранительной деятельности. Ее введению в правовой оборот препятствует пока действующая система способов криминалистической идентификации: по материально фиксированным отображениям; по идеальным образам (мысленному отображению объекта в памяти человека); по описанию признаков; целого по частям.

Представляется, что указанные формы не могут быть в полной мере совместимы (с традиционной криминалистической и процессуальной точек зрения) при использовании цифровых доказательств для идентификации. Причинами этого является следующее. Согласно теории криминалистической идентификации, базирующейся на материалистической теории отражения,

[1] Уздяева У. Д. Цифровой профиль гражданина: криминалистическое значение и вопросы безопасности // Интернет-конференции Сибирского юридического университета. URL: https://conf.siblu.ru/cifrovoy-profil-grazhdanina-kriminalisticheskoe-znachenie-i-voprosy-bezopasnosti (дата обращения: 04.03.2024).

любой след есть отражение реально существующего объекта (или его части) в окружающей действительности или в сознании человека (что тоже не устраняет материальности такого следа, поскольку человек и его характеристики не могут не быть материальными). Каждый такой объект идентичен только самому себе, что позволяет его идентифицировать. У материальных следов имеются определенные характеристики: относительная устойчивость, повторяемость при сохранении основных характеристик и т. п. Однако следы в цифровом пространстве обладают совсем иными характеристиками (возможность бесконечного копирования, изменение при этом метаданных, существование только совместно с носителем цифровой информации и др.), что не позволяет их считать следами в традиционном криминалистическом смысле. Но от этого их значение как следов противоправного деяния, как составляющих криминалистического профиля ничуть не уменьшается. Важно однако учитывать, что категория цифрового следа для того, чтобы стать полноценным элементом цифрового профиля физического (или юридического) лица, должна обрести правовое закрепление. В этой связи указанный выше проект Государственного стандарта Республики Беларусь создал такой прецедент, предложив дефиницию цифрового следа как совокупности информации о помещениях и вкладе пользователя во время пребывания в цифровом пространстве [8, с. 258]. В этом контексте нами в полной мере поддерживается позиция отдельных российских ученых о формировании наряду с личным доказыванием (в устной форме) и материальным доказыванием (на бумажных носителях) также технологии цифрового доказывания при работе с цифровыми доказательствами [11, с. 81].

Формированию цифрового профиля в криминалистически значимых целях, возможно, будет способствовать и применение технологий на основе искусственного интеллекта. Одним из направлений в этой сфере является обработка больших массивов данных, в том числе связанных с анализом социальных сетей, данных геолокации и др. Здесь также интересной является мысль А. Л. Осипенко о том, что в рамках законодательства об оперативно-розыскной деятельности имеет смысл подвергнуть правовому закреплению оперативно-розыскные методы, включив в них среди прочего такой метод, как «аналитический поиск» [12, с. 43]. В рамках действующего законодательства Республики Беларусь об оперативно-розыскной деятельности порядок сбора информации по данному направлению вполне может быть проведен в рамках такого оперативно-розыскного мероприятия, как исследование компьютерной информации (статья 24 Закона Республики Беларусь «Об оперативно-розыскной деятельности»)[1].

Если говорить об опыте Китайской Народной Республики, то благодаря системе социального кредита, работающей с использованием алгоритмов искусственного интеллекта, в режиме реального времени поведение физического лица привязывается к его социальному паспорту, который учитывает степень социальной полезности гражданина [13, с. 198]. Важным шагом по оказанию помощи судам в оценке доказательств явилось внедрение так называемой «Системы 206» – «Шанхайской индивидуальной вспомогательной системы для уголовных дел при реализации судебной реформы, ядром которой является судопроизводство», позволяющей также исследовать единичные доказательства и их цепочки, создавать алгоритмы допроса применительно к конкретной ситуации [14, с. 162–164].

Вместе с тем, учитывая особенности работы алгоритмов на основе искусственного интеллекта, следует обратить внимание на одно важное обстоятельство, которое вкупе с вышеизложенными важными свойствами

[1] Об оперативно-розыскной деятельности : Закон Республики Беларусь от 15 июля 2015 г. № 307-З (в ред. Закона Республики Беларусь от 07.02.2023 № 248-З) // ООО «ЮрСпектр». Нац. центр правовой информ. Респ. Беларусь. Минск, 2024 (дата обращения: 20.06.2024).

цифровых следов требует доработки традиционной криминалистической теории доказывания относительно существующих цифровых реалий. Мало того, что цифровые следы не являются следами-отражениями, но, будучи собираемыми с использованием искусственного интеллекта, они с необходимостью будут трансформироваться, дополняться и изменяться согласно полученным алгоритмом искусственного интеллекта требованиям. Таким преобразованиям, к примеру, подвергаются нечеткие снимки с внешних видеокамер для повышения четкости изображения подозреваемого лица. В результате получается не след-отражение, а вновь созданный объект с новой доказательной достоверностью, который вместе с тем может быть использован на практике для оперативной идентификации преступника. Специфичность работы с цифровыми следами посредством искусственного интеллекта позволила отдельным российским ученым в целом поставить вопрос о том, чтобы выделить эту сферу в самостоятельную форму применения специальных знаний [15, с. 592]. С этим следует согласиться и формировать самостоятельную теорию работы с цифровыми доказательствами, несмотря на отдельные мнения об отсутствии единых подходов к данной проблематике, недостатках в разработке криминалистически значимых алгоритмов использования искусственного интеллекта [16, с. 574]. Эти и многие иные аспекты цифровой реальности должны получить должное криминалистическое осмысление и адекватное правовое отражение.

Заключение

Таким образом, по результатам проведенного исследования можно констатировать следующие выводы:

1. Цифровой криминалистический профиль как криминалистическая категория уже известен и теории и практике, однако он еще не стал общеупотребимым, как не стали единообразными и характеристики, входящие в его структуру. По нашему мнению, цифровой профиль как криминалистическая категория представляет собой совокупность криминалистически значимых характеристик лица (прежде всего физического, но, возможно, и юридического), существующих в цифровой форме, собираемых и сохраняемых в качестве динамической модели такого лица в целях их дальнейшего использования для раскрытия, расследования и предупреждения преступлений и административных правонарушений.

2. Источниками цифровой информации о лице, представляющем криминалистический интерес, могут быть социальные сети, цифровые профили лица в системе электронного взаимодействия с государственными органами и иными юридическими лицами, традиционная криминалистически значимая информация о лице в цифровой форме, данные геолокации и др.

3. Цифровой криминалистический профиль может стать новым системообразующим базисом для формирования системы криминалистической регистрации (учетов) по принципу «от лица – к признакам», а не «от признаков – к лицу»;

4. Создание цифрового криминалистического профиля, его использование требуют трансформации категориального аппарата криминалистической доктрины и законодательства, поскольку настоятельно необходимо введение в правовой оборот термина «цифровое доказательство».

5. Использование цифровых доказательств и технологий собирания доказательств на основе искусственного интеллекта повлечет трансформацию традиционной криминалистической теории доказывания, базирующейся на материалистической теории отражения, в пользу разработки критериев оценки достоверности доказательств, существующих в цифровой среде.

СПИСОК ИСТОЧНИКОВ

1. Стащенко С. П. Административные правонарушения, совершаемые в киберпространстве // Вестник Московского университета МВД России. 2020. № 1. С. 198–200.

2. Лозинский О. И. Компьютерная (цифровая) криминалистика (форензика) в эпоху цифровой трансформации экосистемы уголовного процесса // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2023. № 12 (163). С. 115–120.

3. Троицкий А. А. Форензика – криминалистика будущего // Сборник научных статей по итогам Недели Российской науки в Рязанском филиале Московского университета МВД России имени В. Я. Кикотя. Рязань: Рязанский филиал Московского университета МВД России имени В. Я. Кикотя, 2021. С. 782–786.

4. Федотов Н. Н. Форензика – компьютерная криминалистика. М.: Юридический мир, 2007. 432 с.

5. Черкасова Е. С. Понятие и структура криминалистического профиля лица, совершающего преступления против половой свободы и половой неприкосновенности личности // Расследование преступлений: проблемы и пути их решения. 2020. № 1 (27). С. 132–138.

6. Фойгель Е. И. О понятии поисково-криминалистического профиля неустановленного преступника // Пролог: журнал о праве. 2016. № 4 (12). С. 52–55.

7. Аперонова М. А. Криминалистическая характеристика профиля гражданина // Российская наука в современном мире: сборник статей LIV Международной научно-практической конференции. Москва: ООО «Актуальность.РФ», 2023. С. 459–461.

8. Цифровая трансформация. Основные понятия и терминология: сборник статей / редкол.: А. В. Тузиков (пред.) [и др.]; Национальная акадения наук Беларуси, Объединенный институт проблем информатики. Минск: Беларуская навука, 2020. 267 с.

9. Зайцев О. А., Пастухов П. С. Цифровой профиль как элемент информационно-технологической стратегии расследования преступлений // Вестник Пермского университета. Юридические науки. 2022. Вып. 56. С. 281–308.

10. Гаврилов Ю. В., Салеева Ю. Е. Развитие учения о криминалистической регистрации в условиях трансформации преступности // Труды Академии управления России. 2023. № 2 (66). С. 99–105.

11. Зуев С. В. Технологии доказывания участия в преступлении: история развития и перспективы // Правопорядок: история, теория и практика. 2023. № 4 (39). С. 78–82.

12. Осипенко А. Л. Оперативно-розыскная деятельность в информационном обществе: адаптация к условиям цифровой реальности // Научный вестник Омской Академии МВД России. 2019. № 4 (75). С. 38–46.

13. Амиянц К. А. Противодействие преступности с использованием искусственного интеллекта и соблюдение прав человека // Научный электронный журнал «Матрица научного познания». 2019. № 12. С. 194–202.

14. Реховский А. Ф. Китайский опыт использования искусственного интеллекта в уголовном судопроизводстве // Байкальские компаративистские чтения: материалы международной научно-практической конференции. Иркутск: Байкальский государственный университет, 2022. С. 159–167.

15. Пристансков В. Д., Харатишвили А. Д., Евстратова Ю. А. Искусственный интеллект – новая форма использования специальных знаний в расследовании и раскрытии преступлений // Всероссийский криминологический журнал. 2023. Т. 17. № 6. С. 586–596.

16. Афанасьев А. Ю. Искусственный интеллект в уголовном процессе // Юридическая техника. 2021. № 15. С. 571–574.

REFERENCES

1. Stashchenko S. P. Administrative offenses committed in cyberspace // Bulletin of Moscow University of the Ministry of Internal Affairs of Russia. 2020. No. 1. P. 198–200. (In Russ.)

2. Lozinsky O. I. Computer (digital) forensics (forensics) in the era of digital transformation of the ecosystem of the criminal process // Science and education: economy and economics; entrepreneurship; law and management. 2023. No. 12 (163). P. 115–120. (In Russ.)

3. Troitsky A. A. Forensics – criminalistics of the future // Collection of scientific articles based on the results of the Week of Russian Science at the Ryazan branch of the Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot. Ryazan: Ryazan branch of Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot, 2021. P. 782–786. (In Russ.)

4. Fedotov N. N. Forensics – computer criminalistics. M.: Legal World, 2007. 432 p. (In Russ.)

5. Cherkasova E. S. The concept and structure of the forensic profile of a person committing crimes against sexual freedom and sexual integrity of the individual // Investigation of crimes: problems and ways to solve them. 2020. No. 1 (27). P. 132–138. (In Russ.)

6. Foygel E. I. On the concept of search and forensic profile of an unidentified criminal // Prologue: a magazine about law. 2016. No. 4 (12). P. 52–55. (In Russ.)

7. Aperonova M. A. Forensic characteristics of a citizen's profile // Russian science in the modern world: collection of articles of the LIV International Scientific and Practical Conference. Moscow: OOO Aktualnost RF, 2023. P. 459–461. (In Russ.)

8. Digital transformation. Basic concepts and terminology: collection of articles / editorial board: A. V. Tuzikov (pred.) [et al]; National acad. Sciences of Belarus, Ed. Institute of Problems of Informatics. Minsk: Belarusian Science, 2020. 267 p. (In Russ.)

9. Zaitsev O. A., Pastukhov P. S. Digital profile as an element of the information technology strategy for investigating crimes // Bulletin of Perm. University Legal Sciences. 2022. Issue 56. P. 281–308. (In Russ.)

10. Gavrilov Yu. V., Saleeva Yu. E. Development of the doctrine of forensic registration in the context of transformation of crime // Proceedings of the Academy of Management of Russia. 2023. No. 2 (66). P. 99–105. (In Russ.)

11. Zuev S. V. Technologies for proving participation in a crime: history of development and prospects // Law and order: history, theory and practice. 2023. No. 4 (39). P. 78–82. (In Russ.)

12. Osipenko A. L. Operational search activities in the information society: adaptation to the conditions of digital reality // Scientific Bulletin of Omsk Academy of the Ministry of Internal Affairs of Russia. 2019. No. 4 (75). P. 38–46. (In Russ.)

13. Amiyants K. A. Combating crime using artificial intelligence and respecting human rights // Scientific electronic journal "Matrix of Scientific Knowledge". 2019. No. 12. P. 194–202. (In Russ.)

14. Rekhovsky A. F. Chinese experience in using artificial intelligence in criminal proceedings // Baikal comparative readings: Materials of the international scientific and practical conference. Irkutsk: Baikal State University, 2022. P. 159–167. (In Russ.)

15. Pristanskov V. D., Kharatishvili A. D., Evstratova Yu. A. Artificial intelligence is a new form of using special knowledge in the investigation and detection of crimes // All-Russian Journal of Criminology. 2023. Vol. 17. No. 6. P. 586–596. (In Russ.)

16. Afanasiev A. Yu. Artificial intelligence in criminal proceeding. Legal technoligy. 2021. № 15. P. 571–574. (In Russ.)

Информация об авторе:

Б. В. Асаёнок, кандидат юридических наук, доцент.

Information about the author:

B. V. Asayonok, Candidate of Law, Associate Professor.

Статья поступила в редакцию 25.03.2024; одобрена после рецензирования 11.09.2024; принята к публикации 27.09.2024.

The article was submitted 25.03.2024; approved after reviewing 11.09.2024; accepted for publication 27.09.2024.