4. Аминев, Ф. Г. Об организационном аспекте современной технологии всеобщей ДНК-регистрации граждан / Ф. Г. Аминев, А. В. Анисимов // Правовое государство: теория и практика. – 2020. – № 2 (60). – С. 11–19.

5. Якимов, И. Н. Криминалистика. Руководство по уголовной технике И. Н. Якимов. – М.: Изд-во НКВД РСФСР, 1924. – С. 31.

6. Рыжков, И. В. Теоретические основы и современные тенденции организации функционирования натурных коллекций: дисс. …. канд. юрид. наук / И. В. Рыжков. – Волгоград, 2023. – 213 л.

7. Теория информационно-компьютерного обеспечения криминалистической деятельности: монография // Под ред. Е.Р. Россинской. – М.: Проспект, 2022. – 256 с.

ЦИФРОВОЙ ПРОФИЛЬ ФИЗИЧЕСКОГО ЛИЦА КАК САМОСТОЯТЕЛЬНАЯ КРИМИНАЛИСТИЧЕСКАЯ КАТЕГОРИЯ

Асаёнок Б. В.

УО ФПБ «Международный университет «МИТСО»
ул. Казинца, д. 21, к. 3, 220099, г. Минск, Беларусь, boris.asayonok@gmail.com

В данной работе рассматриваются криминалистические подходы к формированию цифрового профиля физического лица в качестве самостоятельной научно-практической категории. Изучается структура данного профиля и его значение в криминалистической науке и криминалистической деятельности. Предлагается авторский взгляд на определение цифрового профиля физического лица, формулируются предложения о системообразующем значении данного профиля в цифровой криминалистической регистрации. Рассматривается структура цифрового профиля с предложением в качестве самостоятельных элементов 3D-модели физического лица и габитоскопических признаков в цифровом виде.

Ключевые слова: криминалистическая регистрация; цифровой профиль; 3D-метрия в криминалистике

Современный человек немалое время проводит в цифровом пространстве. Это связано и с непосредственной рабочей деятельностью, и со сферой потребляемых услуг, и с проведением досуга. Эти и многие иные сферы уже в достаточном виде представлены в цифровом виде, что позволяет человеку осуществлять значительную часть ежедневной коммуникации с окружающим миром именно в цифровой форме. Преступная деятельность как негативная часть социальной активности человека также в значительной мере приобрела цифровые черты. Большое количество преступлений совершается именно и только в цифровом пространстве. К сожалению, этот фактор повышает уровень трансграничного взаимодействия преступных сообществ, затрудняя возможности привлечения виновных лиц к юридической ответственности.

В связи с этим уже более двух десятком лет развивается такое направление криминалистической науки, как киберкриминалистика. Однако формирование данного направления не отменяет традиционной системы криминалистики, которые позволяют систематизировать и структурировать новые знания, полученные в ходе раскрытия и расследования преступлений в цифровом пространстве. Та-

ким образом, многие классические отрасли криминалистической техники и тактики становятся базисом для осмысления цифровой реальности. Так, криминалистическое учение о следах позволяет развитию категории «цифровой след», в русле организации и тактики отдельных следственных действий (преимущественно речь идет пока об осмотре и обыске) формируются криминалистические рекомендации о работе с цифровыми следами. Организация и тактики назначение и проведения экспертизы как наиболее развитое направление позволяет в полной мере систематизировать вопросы извлечения новой криминалистически значимой информации из цифровых следов и их носителей.

Пребывание в цифровом пространстве, также как и в материальном мире, оставляет многочисленные следы, в том числе и имеющие значение для раскрытия, расследования и предупреждения преступлений. Представляется важным систематизировать их изучение не только в контексте вышеперечисленных отраслей криминалистики, но и в рамках 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 и коллекционной). Однако признание за цифровой реальностью и цифровыми следами самостоятельного значения в качестве криминалистически значимых категорий требует и новых подходов к системе организации криминалистических и оперативных учетов.

Речь идет, прежде всего, о криминалистическом (и оперативно-розыскном) профилировании физического лица. Конечно же, профилированию могут подвергаться и юридические лица. К примеру, это имеет достаточно высокое значение при изучении субъектов экономической деятельности, при выявлении и пресечении таможенных правонарушений в рамках внешнеэкономической деятельности.

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, что, однако, не препятствует возможностям раскрыть его содержание с позиций криминалистической доктрины.

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.

По мнению отдельных авторов, рассматриваемый с криминалистических позиций, цифровой профиль может включать в себя следующие компоненты:

Сам цифровой профиль содержит группы 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 [2, с. 305].

Но, как видится, роль цифрового профиля может быть более значимой. Он может явиться системообразующим фактором, влияющим на построение всей системы криминалистических учетов. Не вызывает сомнения, что объем данный о физическом лице в цифровой форме будет только расти. И если в основу построения криминалистических учетов вновь ввести принцип построения – не от криминалистически значимого признака к человеку, а от человека – к признаку. И если позволить такой системе действовать в режиме постоянного накопления цифровой информации о конкретном человеке, попавшем в сферу внимания правоохранительных органов, то это позволит формировать динамическое цифровое досье (криминалистический цифровой профиль), который может давать требуемую информацию в динамике развития изучаемого объекта.

Однако эти элементы представляются недостаточными для того, чтобы цифровой профиль стал многоуровневой системой идентификации физического лица, пригодной, в том числе, и для традиционных криминалистических исследований. Для этого, как видится, укоренение должно приобрести 3D-моделирование (в контексте 3D-фотосъемки) физического лица, попавшего в сферу внимания правоохранительных органов. Такое моделирование со временем может заменить собой всю систему сигнателических снимков физического лица в опознавательных целях. Оно с эффективностью может использоваться не только в розыскных и опознавательных целях, но и для формирования банка данных моделей статистов для проведения опознания в цифровой форме. Эти модели удобны с точки зрения безопасности опознающих лиц, четкой локации идентификационных признаков (особые и броские приметы), возможности присоединения к ним совокупности иных признаков в качестве сопутствующих баз данных (следы пальцев рук, рисунок сетчатки глаз и др.).

Биометрические данные в цифровом профиле возможно совмещать с социометрическими данными из открытых и ограниченных к доступу баз данных, социальных сетей и профилей физического лица, данными геолокации и др.

С учетом этого, цифровой профиль физического лица в криминалистике следует определить как совокупность криминалистически значимых данных о

физическом лице в цифровой форме (биометрических, социометрических, информации из социальных сетей и др.), имеющих значение для его криминалистической регистрации, а также использования в процессе раскрытия, расследования и предупреждения преступлений.

Формированию цифрового профиля в криминалистически значимых целях может способствовать и применение технологий на основе искусственного интеллекта. Но в настоящее время здесь наметился ряд тенденций, который следует учитывать в целом при использовании таких технологий, доступных в открытой форме. Искусственный интеллект, несмотря на способности быстрой обработки больших массивов данных, не в состоянии выйти за пределы своего «обучения» (это касается, в том числе рамок времени его «обучения», когда создают ограничения на учет тех данных, которые возникли после «обучения»). Столкнувшись с вопросом, который находится вне рамок его досягаемости, искусственный интеллект может выдавать решения, которые соответствуют его предыдущему опыту общения с клиентом, который сформулировал вопрос. То есть в основу ответа на запрос будут положены субъективные предпочтения клиента.

Кроме того, искусственному интеллекту пока недоступны вопросы морального характера, сложны для понимания вопросы юридической квалификации деяний. Имеются мнения, что искусственный интеллект может являться средством манипулирования сознанием лица, которое его использует при принятии решений. Все эти вопросы, конечно же, требуют дальнейшего изучения. Однако следует обратить внимание на то, что искусственный интеллект – всего лишь одно из средств, при помощи которого человек познает и преобразует окружающую реальность (в том числе, реальность диады «преступление-расследование»). И именно поэтому его следует рассматривать не как универсальное, а как однопорядковое с иными криминалистическое средство, хотя и с очень перспективными возможностями. В частности, уже подтверждена высокая значимость программ на основе искусственного интеллекта при поиске в социальных сетях криминалистически значимой информации, поиске и распознании признаков внешности физических лиц, представляющих интерес для правоохранительных органов и др.

Библиографический список

1. Сценарии использования инфраструктуры Цифрового профиля [Электронный ресурс]. Режим доступа: https://digital.gov.ru/uploaded/presentations/stsenarii-ispolzovaniya-infrastrukturyi-tsp-13_w6nhiEs.pdf?utm_referrer=https%3a%2f%2f www.google.com%2f – Дата доступа: 24.03.2023.

2. Зайцев, О. А. Цифровой профиль как элемент информационно-технологической стратегии расследования преступлений / О. А. Зайцев, П. С. Пастухов // Вестн. Перм. ун-та. Юрид. науки. – 2022. – Вып. 56. – С. 281–308.