



## КРИМИНАЛИСТИКА, ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ

---

---

УДК 351.755.6:004.056

**А.И. Бородич**, кандидат юридических наук, доцент, начальник пограничного факультета Института национальной безопасности Республики Беларусь;  
**Н.А. Вашкевич**, старший научный сотрудник научно-исследовательской лаборатории общих криминалистических и автотехнических исследований научно-оперативного отдела криминалистических исследований Научно-практического центра Государственного комитета судебных экспертиз Республики Беларусь;  
**П.И. Жестков**, начальник управления профессионально-должностной подготовки главного управления идеологической работы и кадрового обеспечения Государственного пограничного комитета Республики Беларусь;  
**С.А. Шведова**, начальник отделения планирования управления режима и организационного обеспечения опознания «Минск» Государственного пограничного комитета Республики Беларусь

### ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ЭЛЕКТРОННЫХ ПАСПОРТОВ И АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПРОВЕРКИ ДОКУМЕНТОВ

*Окончание. Начало в № 2 (26) за 2013 г.*

В настоящее время во многих странах для защиты персональных данных электронных паспортов используются биометрические технологии. Однако до сих пор в мире не принят единый стандарт для паспортов нового поколения: одни страны в тестовом режиме вводят в чипы отпечатки пальцев, другие – изображение радужной оболочки глаза, требования к биометрическим характеристикам в разных странах неодинаковы. Поэтому вопросы использования биометрических технологий для защиты персональных данных электронных паспортов и автоматизированной системы проверки документов в пунктах пропуска через границу по-прежнему остаются актуальными. В статье предложены рекомендации, которые могут быть полезны при введении электронных паспортов в Республике Беларусь.

*Ключевые слова:* биометрика, электронные паспорта, машиночитываемые паспорта, пограничный контроль.

С целью единообразного понимания терминов и определений в контексте исследуемой проблемы мы приведем их определение.

Биометрика – область знаний, использующая методы измерения физических характеристик, формулирования персональных поведенческих черт человека и их использования для идентификации или аутентификации человека [1, с. 8]. В отечественной литературе в качестве синонима часто используется термин «биометрия», но он имеет иное значение. Биометрия – раздел биологии, основные задачи которого – планирование количественных биологических экспериментов и обработка результатов методами математической статистики. В биометрике учитывается различие между терминами «идентификация», «аутентификация» и «верификация».

Идентификация (биометрическая) – это процедура, базирующаяся на технологии распознавания образов и предназначенная для однозначного определения личности человека на основе его биометрических характеристик при сравнении их с заданными [1, с. 231]. Аутентификация – подтверждение идентичности представленного образца эталону, хранящемуся в памяти системы распознавания; аутентификация реализуется на основе проверки утверждения о том, что представленный образец есть именно тот, за кого он себя выдает [1, с. 229]. Верификация – дополнительная проверка результата распознавания с целью установления истинности этого результата; верификация реализуется аналогично аутентификации [1, с. 230].

Таким образом, в процессе идентификации система сравнивает один образец со многими. Идентификационная система спрашивает: «Вы кто?» В процессе аутентификации или верификации система сравнивает один образец с одним. Такая система спрашивает: «Вы действительно тот, за кого себя выдаете?»

Биометрическая технология – это отрасль (науки и производства), использующая методы и технические средства получения и использования биометрических данных человека в целях его идентификации [1, с. 230]. Биометрическая характеристика человека – измеряемая физическая характеристика человека или его персональная поведенческая черта [1, с. 13].

Используемые в настоящее время паспорта можно условно разделить на три основных вида: немашиносчитываемые (паспорта старого образца), машиносчитываемые (паспорта нового образца) и электронные (паспорта нового поколения).

Знакомая всем форма паспорта с фотографией появилась в начале XX в. Толчком к массовому появлению паспортов послужила Первая мировая война, во время которой правительства европейских стран усилили пограничный контроль в целях безопасности. В 1920 г. Лига Наций провела специальную конференцию по паспортам и проездным документам. Принципы паспортной системы были определены и на последующих конференциях, прошедших в 1926 и 1927 гг. В результате была принята единая концепция нового паспорта. Так появились обычные (немашиносчитываемые) паспорта с фотографией.

Немашиносчитываемый паспорт – паспорт, в котором отсутствует машиносчитываемая зона. На сегодняшний день в мире осталось четыре страны, паспорта которых не имеют такой зоны [2, с. 30–40].

7 декабря 1944 г. в Чикаго была подписана Международная конвенция о гражданской авиации (Чикагская конвенция). Согласно конвенции создавалась Международная организация гражданской авиации (International Civil Aviation Organization (ICAO)), при которой был организован комитет. Перед комитетом была поставлена задача по разработке формата паспортной книжки, информацию с которого могла бы считать машина. Это было необходимо для сокращения времени, затрачиваемого на проверку документов. Комитет выработал несколько рекомендаций, включая использование оптического распознавания символов в качестве основной технологии автоматического ввода данных. Так появились машиносчитываемые паспорта, получившие в мире наибольшее распространение.

Машиносчитываемый паспорт – паспорт в форме отдельной карточки или паспортной книжки, удобочитаемый как визуально, так и с помощью методов оптического распознавания знаков.

На протяжении последних 40 лет ICAO является лидером по разработке спецификаций – стандартов для проездных документов, носящих рекомендательный характер. Однако все страны – члены ICAO относятся к подобным спецификациям как к стандартам и в своих странах, как правило, вводят внутренние стандарты, дублирующие спецификации ICAO. В странах, где отсутствуют государственные стандарты, применяются спецификации ICAO.

В 1980 г. эти рекомендации нашли отражение в документе, получившем название Doc9303 «Машиносчитываемые проездные документы». В 1997 г. группа Технического совета по машиносчитываемым проездным документам при ICAO значительно переработала этот документ, разделив его на три части – паспорта, визы и идентификационные карты. В 2006 г. первая часть документа Doc9303, касающаяся паспортов, была разбита на два тома. В первый том вошла информация по оптически считываемым (машиносчитываемым) паспортам, а во второй – по электронным.

Электронный паспорт – машиносчитываемый электронный ID-документ, в который имплантирован RFID-чип.

Введение электронных паспортов вызвано необходимостью совершенствования процесса идентификации личности, дальнейшего повышения защиты документов от подделки, возможностью автоматизированного считывания данных с микрочипа. Наличие электронных паспортов позволяет использовать электронные ворота, эта система активно развивается и внедряется в США, Великобритании и других странах Европы. В результате существенно ускоряется процесс проверки документов, а органы, осуществляющие пограничный контроль, получают доступ ко всей информации, связанной с перемещением пассажира, которая размещается в чипе. Кроме того, использование электронных паспортов способствует повышению эффективности борьбы с терроризмом и нелегальной миграцией.

На первом этапе внедрения электронных паспортов в чип вносили информацию, размещенную в машиносчитываемой зоне, и двухмерную цифровую фотографию, отвечающую стандарту, определенному в ISO/IEC 19794-5.

1 ноября 2005 г. в Германии, первой из стран Европейского союза, началась выдача электронных паспортов. В 2006–2007 гг. к этому процессу присоединились все страны ЕС.

До 1 апреля 2010 г. согласно рекомендациям ICAO 190 государств – членов этой организации взяли на себя обязательства дополнительно включать в свои паспорта, визы и другие официальные проездные документы биометрические характеристики: отпечатки пальцев и (или) изображение радужной оболочки глаза. Следует отметить, что ICAO допускает также необязательное включение в чип других биометрических характеристик и иной информации, необходимой для проверки аутентичности владельца документа.

В литературе в качестве синонима термина «электронный паспорт» часто используется термин «биометрический паспорт». Однако не все авторы с этим согласны. Это связано с тем, что ведущие страны мира разделили программу выпуска электронных паспортов на два этапа. На первом этапе в паспорт имплантируется чип с той же информацией, что и на странице с данными: двухмерная цифровая фотография и персональные данные (их еще именуют первым поколением электронных паспортов). Такие паспорта, по сути, биометрическими не являются. На втором этапе в паспорт имплантируется чип, содержащий биометрические характеристики (отпечатки пальцев и (или) изображение радужной оболоч-

ки глаза). Такие паспорта называют вторым поколением электронных паспортов. В обоих случаях на обложку паспорта наносится один и тот же логотип микросхемы.

Таким образом, в чипе электронного паспорта наряду с персональными данными и двухмерной цифровой фотографией биометрические характеристики могут храниться или отсутствовать. Следует отметить, что память микросхем паспортов первого поколения позволяет при необходимости вводить в них биометрические характеристики без замены чипа. Поэтому для электронных паспортов как первого, так и второго поколения наиболее точно подходит термин «электронный паспорт».

Двухмерная цифровая фотография в качестве основной технологии хранения данных электронных паспортов была выбрана в связи с возможностью бесконтактной проверки данных и вмешательства человека в процесс идентификации. Учитывался и фактор привычки – использование фотографии в документах – это общепринятая практика. Вместе с тем ИСАО признала невозможность полного автоматического распознавания лиц по двухмерной фотографии, так как на нее оказывают сильное влияние освещение, ракурс, расстояние между контролером и проверяемым человеком и т. д. В связи с такой неустойчивостью к внешним воздействиям ошибка автоматического сравнения может достигать 50 %.

Проведенный нами опрос военнослужащих пограничного контроля показал, что при идентификации личности в процессе проверки документов в пунктах пропуска в ряде случаев возникают трудности, например, при идентификации близнецов, детей (их признаки внешности быстро изменяются в связи с ростом организма), женщин (на фотографии они, как правило, с макияжем и красивой прической, а во время проверки – не всегда), лиц монголоидной расы, так как все они похожи. Сложности возникают из-за возрастных изменений признаков внешности, изменений, связанных с некоторыми заболеваниями или проведенными косметологическими операциями.

Трехмерные фотографии более надежны для компьютерных алгоритмов, чем двухмерные. Уровень распознавания лиц по трехмерной фотографии составляет более 90 %.

Следует отметить, что методы получения 3D-изображения лица позволяют одновременно получать и 2D-изображение, поэтому оптимальным является одновременное использование двух источников информации. Российские специалисты предложили не вводить отдельный стандарт для 3D-изображения, а дополнить привычную двухмерную фотографию данными о геометрии лица. Это незначительно увеличивает объем памяти, которую будет занимать информация, хранящаяся в чипе. Так, 3D-изображение занимает без потери качества не более 5 Кб памяти, в то время как 2D-изображение в формате jpeg с максимально допустимой потерей качества занимает в чипе 20 Кб [3, с. 27].

Трехмерное распознавание лиц наряду с другими биометрическими технологиями проходило тестирование во многих странах мира. Так, в январе 2006 г. Т. Хартман, директор по технологиям биометрической идентификации компании UNISYS, главный редактор и один из создателей Международной организации по стандартам по цифровому изображению лица, прокомментировал результаты испытаний следующим образом: «Совместно со Службой иммиграции и пограничного контроля Сингапура в течение прошлого года мы проводили тестирование технологии трехмерного распознавания лица. Аналогичные испытания мы проводим и в других странах. Результаты превзошли все ожидания: трехмерное распознавание лица существенно увеличивает точность автоматического распознавания и, главное, не замедляет, а ускоряет процедуру пограничного контроля и регистрации на рейс, существенно увеличивая надежность идентификации» [4].

Наличие в чипе трехмерной фотографии может существенно облегчить работу спасателей, судмедэкспертов и других специалистов, которые занимаются идентификацией погибших во время катастроф, стихийных бедствий, террористических актов и пр. Однако во вторую часть документа Doc9303 «Машиносчитываемые проездные документы» предлагаемая представителями Российской Федерации технология трехмерного распознавания лиц пока не вошла.

Еще одно применение биометрических технологий, связанных с распознаванием личности по лицу и представляющих большой интерес для специалистов пограничного контроля, – это автоматизация профайлинга – процедуры выяснения скрываемой информации по вербальным и невербальным признакам. Обычно создатели автоматизированных систем распознавания по лицу бьются над тем, чтобы отсеять меняющиеся данные, например ситуативную мимику, и все, что связано с психологическим состоянием и настроением человека. Возможен другой вариант – можно фиксировать отклонения от обычного выражения лица и обращать внимание на произвольные изменения мимики, когда человек отвечает на вопросы. Но пока биометрические системы, автоматизирующие процесс профайлинга, на рынке отсутствуют [5].

В декабре 2004 г. европейская комиссия выпустила свой документ – директиву (ЕС) 2252/2004, которая положила начало работе по созданию электронных паспортов в Европе. Директива определила первую спецификацию по переходу к паспортам нового поколения. В ней отмечалось, что с 28 августа 2006 г. все государства, входящие в Европейский союз, должны начать выдачу электронных паспортов с цифровым изображением лица, вносимым в микрочип. Вторая спецификация директивы была принята 28 июня 2006 г. Она обязывала использовать отпечаток пальца в качестве второй технологии хранения данных электронных документов. Конечный срок для государств по приведению в соответствие своих паспортных программ – 28 июня 2009 г.

Таким образом, в соответствии с рекомендациями ИКАО и Европейского союза на втором этапе создания электронных паспортов в чип рекомендуется вводить отпечатки пальцев. Более 100 стран выбрали отпечатки указательных пальцев обеих рук. При этом использование дактилоскопической информации предполагается только в момент проверки человека, до выдачи документа.

Идентификация по отпечаткам пальцев – наиболее распространенная технология распознавания, вероятность совпадения отпечатков у двух разных людей равна примерно  $10^{-9}$ , т. е. один случай на миллиард [6]. Однако по статистике 5–7 % населения нашей планеты имеют отпечатки пальцев, не поддающиеся машинному считыванию.

Идентификация изображения радужной оболочки глаза происходит по 260 уникальным точкам информации по сравнению с 10–60 точками для других биометрических методов. Вероятность генерации системой одинаковых кодов для двух различных людей составляет примерно  $10^{-78}$ . Для сравнения, численность населения Земли в настоящее время составляет более 7 млрд человек [7, с. 35–39].

Метод идентификации человека по радужной оболочке глаза, основанный на распознавании черно-белого изображения, полученного с помощью инфракрасной подсветки, проходил испытания на территории США, Великобритании, Арабских Эмиратов и других государств. Во время апробации выявились отдельные недостатки этого метода. Так, в видимом диапазоне спектра без дополнительной подсветки особенности радужной оболочки видны недостаточно хорошо. В ИК-области спектра у людей со светлой радужной оболочкой значительно хуже видна структура глаза, необходимая для идентификации. В ИК-области спектра существует возможность подделки изображения радужной оболочки глаза. Для устранения этих недостатков российская компания Iris Machines предложила производить захват изображения как в инфракрасном, так и в видимом диапазоне спектра. Проведенные исследования показали, что применение метода идентификации с использованием информации о цвете радужной оболочки увеличивает надежность системы более чем в 200 раз при идентификации по одному глазу и более чем в 40 000 раз при идентификации сразу по двум глазам. При необходимости система может быть дополнена другими биометрическими характеристиками, например изображением лица человека [8, с. 58–61].

Биометрические технологии повышают эффективность идентификации личности, однако компьютерные программы работают с определенной долей погрешности. Получаемые при каждом процессе распознавания биометрические характеристики хоть незначительно, но отличаются от сохраненных в базе данных.

Как показали исследования, в режиме идентификации при базах данных, содержащих сведения о 1000–2000 человек, некоторые методы (по изображению радужной оболочки глаза, по отпечатку пальца, по 3D-фотографии) могут обеспечить приемлемую точность. При базах данных, содержащих сведения о более чем 2000 человек, ни один из биометрических методов «в чистом виде» не применим для большинства задач, в том числе для задач государственного или межгосударственного масштаба (когда требуется идентификация по базам данных в несколько сотен тысяч или миллионов человек). Например, задача поиска человека с определенными биометрическими характеристиками в государственной базе данных выданных паспортов или виз. Но человека, которого не сможет идентифицировать одна биометрическая система, распознает другая. Таким образом, для увеличения точности идентификации целесообразно использовать несколько биометрических методов одновременно [7]. Наилучшие результаты достигаются, когда идентификация личности осуществляется биометрическими и традиционными методами. Так, цифровая фотография владельца паспорта может использоваться как для автоматизированной проверки документа, так и для визуальной идентификации личности.

1. Кухарев, Г.А. Биометрические системы: методы и средства идентификации личности человека / Г.А. Кухарев. СПб. : Политехника, 2001. 240 с.
2. Балуева, Т. Интеграция и доверие / Т. Балуева // Водяной знак. 2012. № 6. С. 38–40.
3. Кресп, О. Самый защищенный документ / О. Кресп // Стандарт. 2005. № 11. С. 26–28.
4. Паспорта: Россия изменила мировой биометрический стандарт [Электронный ресурс] // CNews : изд. о высоких технологиях. Режим доступа: <http://www.cnews.ru/news/top/index.shtml?2006/01/24/194883>. Дата доступа: 30.01.2012.
5. Вакуленко, А. Аэропорты: зона особого внимания [Электронный ресурс] / А. Вакуленко // Приказано жить! О людях, стихиях и о Земле. Режим доступа: <http://www.zhivi-i.ru/progress/index01.htm>. Дата доступа: 22.02.2013.
6. Панканти, Ш. Биометрия: будущее идентификации / Ш. Панканти, Р.М. Болле, Э. Джейн // Открытые системы. 2000. № 3. С. 17–20.
7. Вакуленко, А. Биометрические методы идентификации личности: обоснованный выбор и внедрение [Электронный ресурс] / А. Вакуленко, А. Юхин // НПО Информ: биометрические системы безопасности. Режим доступа: <http://www.npo-inform.ru/press/biovybor/>. Дата доступа: 04.05.2012.
8. Кузнецов, И. Цвет приходит из России / И. Кузнецов // Водяной знак. 2011. № 4. С. 58–61.

Дата поступления в редакцию: 24.09.13

*A.I. Borodich, PhD of law, associate professor, head of the department of border of the Institute of Homeland Security of the Republic of Belarus; N.A. Vashkevich, senior staff scientist of the Scientific Research Laboratory of general forensic and auto-*

*technical research of the research department of forensic science research of the Scientific and Practical Centre of the State Committee of forensic examination of the Republic of Belarus; P.I. Zhestkov, head of the department of professional and vocational preparation of the second department of prime responsibility of the State Border Committee of the Republic of Belarus; S.A. Shvedova, head of the department of planning, management, security and organizational support of 'Minsk' border control brigade of the State Border Committee of the Republic of Belarus*

USING BIOMETRIC TECHNOLOGIES FOR PROTECTION OF E-PASSPORT PERSONAL DATA AND AUTOMATED DOCUMENT VERIFICATION SYSTEM

*Currently, in many countries the biometric technologies are used to protect e-passport personal data. However, until now, there is no accepted unique standard for the next generation of passports in the world; some countries introduce fingerprints into chips in the test mode, others – the iris image, the requirements for biometric characteristics in different countries are different, too. Therefore, the issues of using biometric technologies to protect e-passport personal data and the document check automated system at checkpoints on the State Border are still relevant. The article offers recommendations that may be useful for the introduction of e-passports in the Republic of Belarus.*

*Keywords: biometrics, e-passports, machine-readable passports, border control.*

УДК 343.983.3:53

**А.В. Дулов**, доктор юридических наук, профессор, заслуженный деятель науки Республики Беларусь, профессор кафедры криминалистики Белорусского государственного университета;

**К.С. Егоров**, кандидат юридических наук, ведущий эксперт Центра судебных экспертиз и криминалистики Министерства юстиции Республики Беларусь

**ЗВУКОВОЙ СЛЕД ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ:  
ПОНЯТИЕ И КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМЫЕ СВОЙСТВА**

*Окончание. Начало в № 2 (26) за 2013 г.*

*Анализируется и уточняется понятие «звуковой след преступной деятельности». На основе последовательного применения концепции логических родо-видовых отношений и существенных видообразующих признаков из родового понятия «след» выводится формулировка научно обоснованного определения понятия «звуковой след преступной деятельности». Предложенные определения понятий служат основой для разработки научно-методической базы при решении ряда основополагающих задач криминалистической экспертизы звукозаписей в современных условиях развития науки криминалистики и новых информационных технологий.*

*Ключевые слова: преступная деятельность, следы преступления, звуковой след, голосовая информация, речевая информация, объекты – источники звука, криминалистические свойства, след преступной деятельности.*

Возможность использования следов-отражений различных объектов для раскрытия и расследования преступлений была отмечена еще В.И. Корюкиным: «Для того, чтобы узнать о событии, мы должны выделить связанные с ним изменения. Связь изменений с событием существует объективно» [1, с. 42–43].

Основоположник теории криминалистики Р.С. Белкин для научно обоснованного применения этой закономерности к деятельности по расследованию преступлений также использовал существующую методологию ленинской теории отражения [2–4]. Криминалистический смысл теории отражения в наиболее сконцентрированном виде он выразил в том, что «событие преступления есть один из материальных процессов действительности. Как таковой он находится в закономерной связи и взаимообусловленности с другими процессами, событиями и явлениями. Эти процессы составляют ту среду, в которой совершается преступление. Как и всякий материальный процесс, преступление взаимодействует со средой, и одной из сторон такого взаимодействия служит отражение преступления в окружающей среде, выражающееся в ее изменениях, адекватно отражающих процесс преступной деятельности» [4, с. 52–53].

В общем случае криминалистика как специальная юридическая наука о теории, средствах и методах организации эффективной борьбы с преступностью изучает закономерности возникновения следов различных объектов, обнаружения следов, фиксации следов, исследования различных объектов, в том числе по их частям и следам, оценки и использования вещественных доказательств в процессе доказывания. При этом необходимо учитывать влияние результатов научно-технического прогресса, к числу которых относится и расширение следовой картины совершаемых преступлений, появление новых, нетрадиционных следов, могущих быть использованными в целях раскрытия и расследования преступлений, доказывания виновности злоумышленников [3, с. 219]. Не является исключением и возможность внедрения и использования новых методов криминалистического использования звуковых следов.

Проведенный в работе Н.А. Костикова анализ также свидетельствует о том, что до настоящего времени ученые-криминалисты и практические специалисты не пришли к единому научному определению понятия «звуковой след преступной деятельности» [5]. Ниже будут рассмотрены их различные точки зрения, определение же понятия «звуковой след преступной деятельности» будет уточнено на основе применения новых видообразующих признаков, удовлетворяющих современным требованиям, предъ-