Введение

B1. История возникновения и развития

Успехи в вопросах биометрической идентификации личности базируются на достижениях бионики (от греч. Bion — элемент жизни, буквально — живущий) — области науки, изучающей методы измерения физических характеристик и поведенческих черт человека для последующей идентификации и аутентификации личности, а именно науки, пограничной между биологией и техникой, решающей инженерные задачи на основе анализа структуры и жизнедеятельности организмов.

Бионика тесно связана с биологией, физикой, химией, кибернетикой и инженерными науками — электроникой, навигацией, связью, морским делом и др. Прикладная бионика — наука, которая сочетает в себе биологию и технику. Без этой науки невозможно представить технический прогресс во многих сферах деятельности человека.

Ученые всегда пытались систематизировать и объяснить различные признаки и свойства особей, проявляющихся в экспериментах. В конце XIX века ученые Фрэнсис Гальтон и Карл Пирсон, изучая закономерности в наследственности людей, применили методы вариационной статистики к анализу различных особей и положили начало науке биометрия.

Биометрические методы распознавания применяются человечеством на протяжении всей его истории, область их применения лежит в плоскости *безопасности и контроля* [1–11]. Чаще всего мы узнаём знакомых людей именно с их помощью — по лицу, голосу или походке. С давних времен *биометрические характеристики* использовались в повседневной жизни. Особенности строения человеческого тела, лежащие в основе первых биометрических доктрин, внесли огромный вклад в развитие криминалистики. В конце XIX века для идентификации преступников в Европе использовалась процедура бертильонажа. Её создал Альфонс Бертильон, сотрудник парижской префектуры, занимавшийся регистрацией пре-

ступников, который и предложил использовать новую систему идентификации собственной разработки в 1879 году. Система учитывала практически неподверженные изменениям со временем антропометрические измерения: длину тела, длину каждой руки, а также словесный портрет, составленный по определённым правилам, специальную фотографию в анфас и профиль, а также описание особых примет преступника. С 1890 года бертильонаж применялся в большинстве стран мира, однако в начале XX века был вытеснен дактилоскопией, отличавшейся простотой и точностью измерений. В начале XX века англичанином Эдвардом Генри был предложен способ, благодаря которому идентификация по отпечаткам занимала несколько минут. Через 10 лет система отпечатков стала практиковаться во всей Европе, а с конца прошлого века в связи с развитием техники возникла возможность формализовать алгоритмы распознавания человека по его внешнему виду или особенностям поведения.

До 2011 года возможности биометрии использовались преимущественно криминалистами и спецслужбами для выявления преступников, защиты государственной тайны и сверхважной коммерческой информации, причём объёмы информации, с которыми приходилось иметь дело, измеряются миллионами записей, и есть даже специальный термин для обозначения таких систем — АДИС (автоматизированная дактилоскопическая идентификационная система). Биометрические технологии также применяются и в других сферах, например для поиска разыскиваемых субъектов в потоке людей по внешнему виду.

Под биометрическими технологиями понимают автоматические или автоматизированные методы распознавания личности человека по его биологическим характеристикам или проявлениям. В настоящее время стала очевидной необходимость точной идентификации в местах массового скопления людей, при контроле пропусков и сверке документов. В первую очередь проблема коснулась безопасности транспортных систем — аэропортов, вокзалов, морских портов, метрополитена, а также государственных и межгосударственных систем — паспортно-визовых, таможенных, миграционных и оперативных служб. Обычных паспортов и фейс-контроля стало явно недостаточно. Все надежды теперь связаны с использованием биометрических технологий, позволяющих проверять личности огромного количества людей.

Для идентификации можно применять различные биометрической характеристики человека (БХЧ). Их подразделяют на статические, связанные с его физическими характеристиками, например

отпечатком пальца или формой уха, и динамические или поведенческие, связанные с особенностями выполнения человеком каких-либо действий, например походка. Наиболее развитыми на данный момент технологиями являются распознавание по отпечатку пальца, радужной оболочке глаза и двумерному (плоскому, как на фотографии) изображению лица. Причём дактилоскопическая идентификация в настоящий момент по применимости и доступности с финансовой точки зрения превосходит все другие. Перечень используемых биометрических признаков человека постоянно расширяется.

В нынешнее время биометрия стала более обширной и являются средством дополнительной защиты для технических средств или же элементом безопасности, который применяется в системах контроля и управления доступом, для пропуска на охраняемую территорию, помещения и т. д. [4, 5, 9, 11].

Используя новейшие биометрические решения, пользователи будут иметь все больше и больше возможностей для комбинирования удобства с безопасностью. С ростом популярности моделей биометрической верификации интеграторам выдвигаются новые требования к обеспечению безопасности. Биометрия в настоящее время переживает период бурного развития. Большое количество нормативных нормативных актов, научных исследований и публикаций по данной теме свидетельствует о повышенном интересе к данному направлению.

B2. Области применения. Перспективы

С 2011 года, после террористических атак на США, ситуация с применением биометрических технологий начала резко меняться. Сначала биометрическими системами доступа оборудовали аэропорты, крупные торговые центры и другие места скопления людей. Повышенный спрос спровоцировал активность научных исследований в этой области, что, в свою очередь, привело к появлению новых устройств и целых технологий.

В настоящее время биометрия применяется для распознавания личности во многих сферах деятельности, таких как контроль физического доступа и доступа к компьютеру, в правоохранительных органах, при голосовании, пересечении границы, в системе социального обеспечения и при выдаче водительских прав [12].

Основными сферами приложений биометрической системы доступа являются:

- правительственный и военный сектор;
- правоохранительные органы и судебная экспертиза;
- таможенная и иммиграционная службы;

- финансовый сектор;
- сектор туризма и др.

Основными областями приложений биометрической системы доступа являются:

- контроль доступа в системах информационной безопасности, особенно в государственных и правительственных учреждениях;
- контроль физического доступа в государственных и правительственных учреждениях;
- системы информационной безопасности (физический и удаленный доступ).

Главными тенденциями внедрения биометрического контроля доступа в различных отраслях рынка являются:

- *государство*, промышленность быстро движется к решениям, которые используют сенсоры для считывания отпечатков пальцев, способные проверять подлинность водительского удостоверения, паспорта или другого удостоверения личности, а также личности, у которой документ находится;
- *корпорации*, в современной бизнес-среде биометрия облегчает защиту документов, требуя от пользователей аутентификации с помощью карты, пропуска или отпечатка пальца. Предпринимательская среда также, вероятно, станет одной из первых отраслей, где будет активно использоваться биометрия в мобильных устройствах;
- *здравоохранение*, биометрия будет играть большую роль в больницах при регистрации больных, в управлении очередями посетителей, защите конфиденциальности информации пациентов, при осуществлении платежей и обеспечении раздачи лекарств без утечки наркотических препаратов, а также при решении других задач повседневной деятельности;
- *банки*, биометрия будет продолжать распространяться в банковской отрасли по всему миру для повышения качества обслуживания клиентов при одновременном повышении безопасности банкоматов и других объектов;
- *транспорт*, биометрические системы дадут интеграторам возможность помочь клиентам в транспортной отрасли увеличить как безопасность, так и прибыль;
- *розничная торговля, интегрированные биометрические считыватели* улучшат проверку личности владельцев карт, используемых в платежных системах и программах лояльности, увеличат их функциональность и эффективность контроля доступа;

высшее образование, новые типы решений для обеспечения обучения и безопасности, контроля доступа в лаборатории и другие важны объекты, в которых проводят эксперименты с опасными химическими веществами или биологическими и радиоактивными материалами;

защита информации, разработка систем биометрической идентификация и аутентификации в сфере информационной безопасности по двум направлениям: физическая защита объектов информатизации, при которой к системе обработки допускается только нужные сотрудники, и допуск к информационным ресурсам компьютера конкретного сотрудника.

Несмотря на большое разнообразие областей приложений биометрических систем, можно выделить два главных направления их применения:

- криминалистика (судебно-медицинские экспертизы);
- безопасность информации (защита государственной, банковской и коммерческой тайны, личные и другие данные и сведения) как при защите контролируемых зон объектов информатизации, так и при ограничении доступа к информации в сетях и конкретных ЭВМ.

Целью настоящей монографии является обобщение, анализ, систематизация и классификация базовых схем и основных элементов систем идентификации личности в криминалистике и защите информации, сравнение эффективности различных биотехнологий, определение направлений повышения эффективности биоидентификации личности за счет внедрения мультибиометрических технологий.

1 Биометрическая идентификация: методы и характеристики

1.1. Основные понятия и определения в идентификации

1.1.1. Понятие и научные основы криминалистической идентификации

В процессе расследования преступлений возникает необходимость установить по следам и иным отображениям связь человека, предмета, иного объекта с расследуемым событием, по результатам отображения идентифицировать объект, оставивший это отображение. Понятия «объект» и «отображение» трактуются достаточно широко [13–17].

Под *объектом* понимают человека, предметы его одежды и обувь, орудия преступления, транспортные средства, оружие, инструменты и т. п. В качестве отображений фигурируют различные следы (живые лица, мертвые тела или их части, вещественные доказательства биологического происхождения: кровь, волосы, кусочки органов и тканей и т. д.), документы, фотоснимки, части объектов, мысленные образы.

Идентифицировать объект — значит установить (выявить) его тождественность с самим собой в разные периоды времени или в разных его состояниях, используя для этих целей оставленные им отображения.

Любое преступление совершается в условиях реальной действительности, и при этом в окружающей среде, где совершается то или иное преступление, неизбежно образуются различные следы (отображения) в силу всеобщего свойства материи — свойства отражения. И при раскрытии преступлений часто возникает необходимость определить по следам или иным отображениям связь человека, предмета (орудия взлома) или иного объекта с расследуемым событием. Идентифицировать, отождествлять — значит методом сравнительного исследования установить, не являются ли определенный объект искомым.

Криминалистическая идентификация — это процесс сравнительного исследования свойств (признаков) объектов, отображенных в следах и в сравнительных материалах с целью установления их тождества по совокупности общих и частных признаков для последующего установления единичного объекта и его связей с расследуемым событием и участвующими в нем лицами [15].

Все объекты делятся на *идентифицируемые* (отождествляемые) и *идентифицирующие* (отождествляющие). В свою очередь идентифицируемые объекты подразделяются на *искомые* и *проверяемые*. А идентифицирующие объекты делятся на *исследуемые* (называемые также следами или объектами неизвестного происхождения) и *образцы для сравнения* (объекты известного происхождения).

Из определений следует, что прежде всего идентификация является процессом исследования. Раз она является процессом исследования, то в нем участвуют определенные лица, которые устанавливают данный единичный конкретный объект. Их принято называть субъектами криминалистической идентификации. Ими могут быть различные участники уголовного процесса: следователь, дознаватель, судья, эксперт, потерпевший, подозреваемые и т. п. Каждый из них решает задачи идентификации в соответствии со своими процессуальным положением и средствами, а также в соответствии с законом.

В криминалистической идентификации изучаются не все свойства и признаки, а главным образом их внешние признаки, особенности внешнего строения объектов. Эти особенности внешнего строения объектов при определенных условиях отображаются на другие объекты. Например, особенности внешности человека — в памяти другого человека, на фотографии и т. д.

Отображения объектов существуют в различных формах, а именно:

- отображение в виде мысленных образов, возникающих в сознании людей как результат зрительных или иных восприятий (приметы преступника в памяти потерпевшего, особенности звука выстрела);
- отображение в виде описания, рисунков, сделанных в момент или после зрительного восприятия объектов самими наблюдаемыми или по их показаниям другими лицами (следователем, художником и т. п.) (ориентировки, субъективные портреты);
- отображения как фиксирование воспроизведения выработанных навыков, например навыков письменной речи и почерка в рукописях, способа преступных действий в окружающей среде;

- фотографические отображения и отображения в виде механических записей человеческой речи (фонограммы);
- отображение в виде частей предметов и частиц вещества (части орудия взлома, осколки фарного стекла на месте происшествия);
- отображение в виде различного вида следов (следы рук, ног, орудий взлома, транспортных средств).

В зависимости от того, какое использовалось отображение для идентификации, определяется вид и самой идентификации.

В зависимости от характера отображения признаков объекта, тождество которого устанавливается, различают четыре вида криминалистической идентификации.

Идентификация объектов по мысленному образу. Широко используется в практике расследования преступлений при проведении следственного действия — предъявление для опознания [13].

Идентификация объекта по его описанию. Используется главным образом для розыска преступников и похищенных вещей, установления неопознанных трупов, а также в криминалистических учетах.

Идентификация объектов по их материально-фиксированным отображениям (следам, фотоснимкам, рукописям и т. п.) — наиболее частый случай криминалистической идентификации, осуществляемый в процессе проведения криминалистических экспертиз.

Идентификация объекта по его частям. Проводится в случаях, когда возникает необходимость установить, что эти части до разрушения (разделения) объекта составляли единое целое. Например, по осколкам фарного стекла, обнаруженным на месте происшествия и изъятым из фары автомобиля, идентифицируется данный автомобиль как участник этого происшествия.

Научной основой криминалистической идентификации являются положения теории об индивидуальности и относительной устойчивости объектов материального мира и их способности отражать свои признаки на других объектах.

Индивидуальность объекта выражается в наличии у него неповторимой совокупности признаков, которых нет у другого подобного объекта [15–17]. Такими признаками для предмета, вещи являются размеры, форма, цвет, вес, структура материала, рельеф поверхности и иные признаки; для человека — особенности фигуры, строение головы, лица и конечностей, физиологическое особенности организма, особенности психики, поведения, навыки и т. д. Раз объекты материального мира индивидуальны, тождественны самим

себе, то им, следовательно, свойственны индивидуальные признаки и свойства. В свою очередь эти признаки объектов отображаются на других объектах. Отображения, стало быть, также являются индивидуальными.

С другой стороны, все материальные объекты подвергаются непрерывным изменениям (человек стареет, например, и т. д.). Хотя объекты изменяются постоянно, но в течение определенного времени сохраняют наиболее устойчивую часть своих признаков, которые позволяют осуществить идентификацию. Свойство материальных объектов сохранять, несмотря на изменения, совокупность своих признаков называется относительной устойчивостью.

Виды криминалистической идентификации. В зависимости от оснований классификации идентификация подразделяется на следующие виды:

- *по правовой природе:*

а) процессуальная, т. е. осуществляемая в рамках уголовно-процессуального закона;

б) не процессуальная, т. е. проводимая при оперативно-розыскных мероприятиях, при составлении криминалистических отчетов;

- *по субъектам проведения* — а) оперативный работник; б) следователь; в) прокурор; г) специалист; д) суд; е) эксперт;
- *по характеру отображений*:

а) идентификация по материально-фиксированным отображениям признаков объектов;

б) отображение по мысленному образу, запечатленному в памяти человека (при опознании).

Особенности криминалистической идентификации:

- применяется в специфической сфере — доказывания;
- цель — установление индивидуального тождества;
- объекты идентификации часто представлены в ничтожно малых количествах и неблагоприятном состоянии;
- использует специфические методы;
- сжатые сроки исследования;
- особый порядок оформления результатов.

Основные принципы криминалистической идентификации:

- строгое разделение объектов идентификации на идентифицируемые и идентифицирующие;
- объекты подразделяются на изменяемые и неизменяемые (отождествление возможно при условии, если объект способен сохранить свои свойства);
- процесс отождествления представляет собой сочетание анализа и синтеза;

- каждый идентификационный признак должен изучаться в динамическом развитии в связи с предшествующими и сопутствующими обстоятельствами;
- вывод о тождестве должен основываться на комплексе согласованных между собой идентификационных признаков.

Идентификационное исследование включает в себя четыре стадии.

1. Стадия предварительного осмотра, в ходе которой эксперт определяет, передано ли ему всё необходимое для исследования, пригодны ли для идентификации предоставленные образцы и что в принципе собой представляют объекты идентификации.

2. На стадии раздельного исследования (аналитической стадии) идентифицируемый и идентифицирующий объекты изучаются отдельно друг от друга. Цель этого этапа — установить как можно больше общих и частных признаков, необходимых для дальнейшего исследования.

3. В ходе следующей стадии — сравнительного исследования — выявляются совпадения и различия в признаках объектов идентификации. Сопоставляют общие признаки, а потом, если они совпадают, переходят к сравнению частных.

4. Оценка — заключительная стадия идентификационного исследования и, пожалуй, самый сложный и ответственный его этап. Трудность состоит в том, что наряду с совпадениями всегда встречаются и некоторые различия, поэтому эксперту приходится решать вопрос об идентификационной значимости совпадающих и различающихся признаков.

1.1.2. Понятие и научные основы идентификации в задаче защиты информации

Идентификация, аутентификация, авторизация и администрирование. Эти понятия взаимосвязаны: сначала определяют имя (логин или номер) — идентификация, затем проверяют пароль (ключ или отпечаток пальца) — аутентификация, и в конце предоставляют доступ — авторизация. Администрирование — это регистрация действий пользователя [1, 18–27].

Согласно ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний», *идентификация* (от лат. identifico — отождествлять) — это процесс опознавания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку. Под идентификацией понимают также присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявля-

емого идентификатора с перечнем присвоенных идентификаторов [19–21].

Биометрическая идентификация — это процесс поиска по базе данных биометрических регистраций, направленный на поиск и возврат идентификатора(ов) биометрического контрольного шаблона, связанного с одним индивидом (ГОСТ ISO/IEC 2382-37-2016) [19–21].

С практической точки зрения процесс идентификации рассматривается как сравнение введенного в систему идентификационного признака (кода) с образцами кодов, хранящимися в памяти системы (поиск и сравнение одного со многими).

Идентификация в биометрической системе проходит в четыре стадии:

- регистрация идентификатора — сведения о физиологической или поведенческой характеристике преобразуются в форму, доступную компьютерным технологиям, и вносятся в память биометрической системы;
- выделение — из вновь предъявленного идентификатора выделяются уникальные признаки, анализируемые системой;
- сравнение — сопоставляются сведения о вновь предъявленном и ранее зарегистрированном идентификаторе;
- решение — выносится заключение о том, совпадают или не совпадают вновь предъявленный идентификатор.

Заключение о совпадении/несовпадении идентификаторов может затем транслироваться другим системам (контроля доступа, защиты информации и т. д.), которые далее действуют на основе полученной информации.

Аутентификация (от греч. $\alpha\upsilon\theta\varepsilon\nu\tau\iota\kappa\acute{o}\varsigma$ — реальный или подлинный) — это процесс опознавания субъекта или объекта путем сравнения введенных идентификационных данных с эталоном (образом), хранящимся в памяти системы для данного субъекта или объекта (ГОСТ Р 51 241-2008). Действие, доказывающее или показывающее бесспорное происхождение или достоверность (ГОСТ ISO/IEC 2382-37-2016 «Информационные технологии. Словарь. Часть 37. Биометрия») [19–21].

С практической точки зрения процесс аутентификации рассматривается как предоставление доказательств, что вы на самом деле есть тот, кем идентифицировались (от слова authentic — истинный, подлинный), т. е. рассматривается как сравнение одного с одним.

Введение в стандарте этих двух терминов связано с тем, что данные понятия близки по смыслу, часто используются не только

в области контроля доступа, но и в информационных системах, в области защиты информации и других сферах.

Различают два вида биометрических систем аутентификации: унимодальные — те, которые используют только одну особенность человека, и мультимодальные (мультибиометрические) — использующие комбинацию унимодальных. В ходе различных исследований было показано, что использование мультимодальных методов аутентификации позволяет увеличить точность работы биометрических систем аутентификации. Слияние нескольких биометрических характеристик объединяет сильные стороны унимодальных биометрических систем и повышает точность распознавания биометрической системы [22, 25].

Авторизация — это процедура предоставления субъекту определенных полномочий и ресурсов в данной системе (проверка о разрешении доступа к запрашиваемому ресурсу). Авторизация устанавливает сферу действия субъекта и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены. Другими словами, авторизация — это предоставление лицу возможностей в соответствие с положенными ему правами или проверка наличия прав при попытке выполнить какое-либо действие. Например, авторизацией являются лицензии на осуществление определённой деятельности.

С процедурами идентификации и авторизации тесно связана процедура администрирования действий пользователя.

Администрирование — это регистрация действий пользователя в сети, включая его попытки доступа к ресурсам.

Аналогично эти термины применяются в компьютерных системах, где традиционно под *идентификацией* понимают получение вашей учетной записи (identity) по username или email; под *аутентификацией* — проверку, что вы знаете пароль от этой учетной записи, а под *авторизацией* — проверку вашей роли в системе и решение о предоставлении доступа к запрошенной странице или ресурсу.

В современных системах существуют более сложные схемы аутентификации и авторизации, использующие различные факторы — информационный, физический и биометрический.

Основные методы аутентификации (парольные, комбинированные, биометрические, информация о пользователе и пользовательские данные) приведены на рис. 1 [18].

Идентификация по запоминаемому коду (информационный фактор, логический фактор знания) осуществляется по коду (паролю, графическому ключу), который должен запомнить человек

Рис. 1. Классификация протоколов аутентификации

(пользователь) и который вводится вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств.

Использование пароля технически просто реализуемо, но с такой же легкостью пароль может быть скомпрометирован, например, шпионской программой или компьютерным вирусом, которые во множестве могут быть загружены на устройства пользователя из Интернета. А когда речь идет об устройствах (например, считыватель PIN-кода) пароль может быть банально подсмотрен.

Идентификация по вещественному коду (физический фактор, фактор владения) выполняется по коду, записанному на физическом носителе (идентификаторе), в качестве которого применяются различные электронные ключи, пластиковые карты, брелоки и т. д.

Каждый из этих способов имеет определенные достоинства и недостатки, но основные отличия связаны с тем, что два вида идентификации (запоминаемый и вещественный) относятся к классу *присвоенных идентификационных признаков*. При этом иденти-