УДК 004.891 *Научная статья* DOI: 10.18287/2223-9537-2023-13-1-55-74

Онтология идентификации человека по движениям тела и лицу в видеонаблюдениях

© 2023, А.Е. Колоденкова

Самарский государственный технический университет, Самара, Россия

Аннотация

В настоящее время разработка моделей и методов распознавания по движениям тела и лицу в видеонаблюдениях является актуальной задачей. Особенно это важно в обеспечении безопасности на объектах с массовым скоплением людей для противодействия преступлениям террористической направленности. В статье приведена классификация основных биометрических признаков и параметров, характеризующих потенциального нарушителя, разработанная для систем контроля безопасности, пропускных систем предприятий. Предложена структурная схема слияния биометрических данных и распознавания нарушителя, которая может лежать в основе разработки систем контроля безопасности. Рассмотрены виды систем и методы распознавания человека по движениям тела и лицу, выявлены их достоинства и недостатки. Отмечено, что для распознавания нарушителя в условиях множества биометрических признаков целесообразно использовать комбинацию методов распознавания. Это позволит принимать правильные решения относительно выявления потенциального нарушителя. В статье сделана попытка рассмотреть основные аспекты, касающиеся распознавания человека по движениям тела и лицу в видеонаблюдениях в целом, в отличие от известных работ, посвящённых отдельным биометрическим признакам.

Ключевые слова: *методы распознавания, биометрические признаки, потенциальный нарушитель, системы контроля безопасности, видеонаблюдения, онтология.*

Цитирование: *Колоденкова А.Е.* Онтология идентификации человека по движениям тела и лицу в видеонаблюдениях // *Онтология проектирования*. 2023. Т.13, №1(47). С.55-74. DOI: 10.18287/2223-9537-2023-13-1-55-74.

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.

Введение

Согласно статистике в Российской Федерации в 2022 г. зарегистрировано 2233 преступления террористического характера и 1566 – экстремистской направленности [1]. С увеличением преступлений террористического характера на стратегических объектах, в учебных заведениях, в различных организациях с массовым скоплением людей главная роль отводится сотрудникам, обеспечивающим внутриобъектовый и пропускной режим [2, 3].

С развитием информационных технологий обеспечение надёжной защиты объектов невозможно без применения систем контроля безопасности (СКБ), основанных на биометрии. СКБ основываются на уникальных характеристиках человека, которые сложно фальсифицировать, и позволяют однозначно распознать конкретного человека. В СКБ существенными биометрическими признаками являются движения тела (походка, жестикуляция, осанка) и мимика (лицо), поскольку их можно наблюдать издалека по видео без прямого контакта с человеком.

Целью настоящей статьи является анализ подходов к распознаванию человека по движениям тела и лицу при выявлении потенциального нарушителя из общей массы людей, а также предложить рекомендации разработчикам систем распознавания нарушителя по видеонаблюдению.

1 Онтология предметной области

Онтология (онтологическая модель) предметной области (ПрО) представляет собой систему, состоящую из набора понятий и отношений между ними. Формальную модель онтологии ПрО можно представить в виде кортежа:

$$O = <X, A, R, F>,$$

где X – конечное множество понятий ПрО; A – конечное множество атрибутов понятий X; R – конечное множество отношений между понятиями, заданной ПрО; F – конечное множество функций интерпретации, заданных отношениями онтологии.

Фрагмент онтологии процесса идентификации нарушителя в виде семантической сети представлен на рисунке 1.

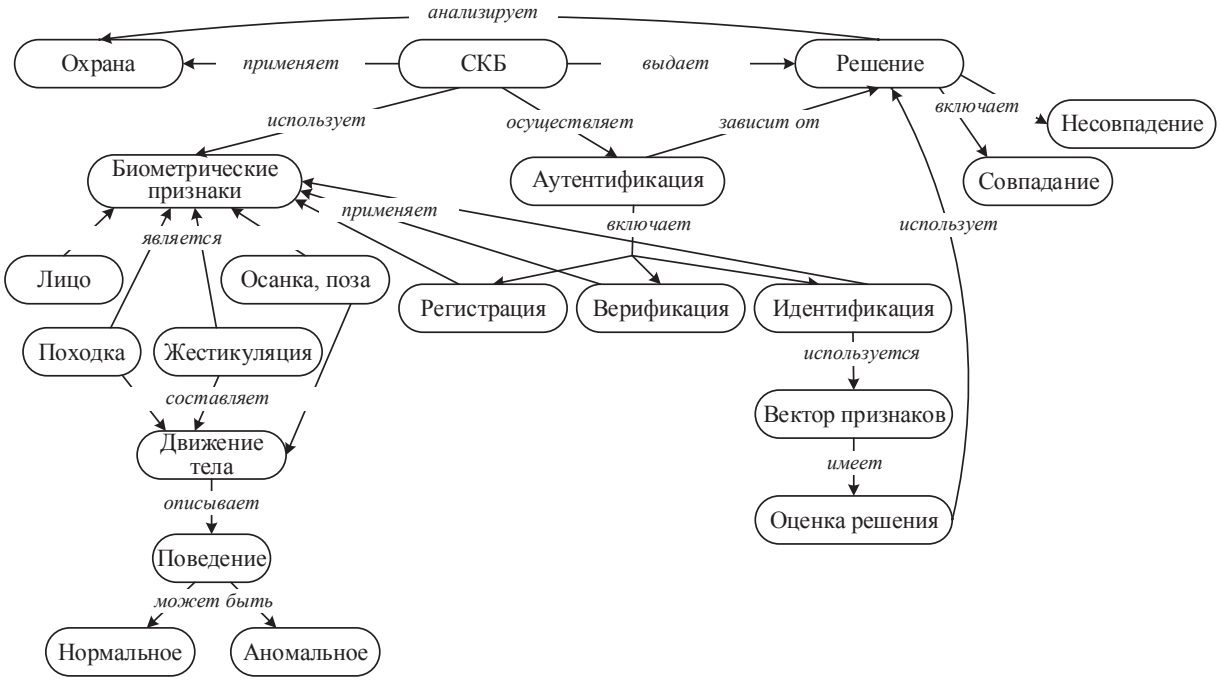

Рисунок 1 – Фрагмент онтологии процесса идентификации нарушителя

ПрО «процесса идентификации нарушителя» включает список понятий, для которых определены атрибуты и отношения. Фрагмент спецификации понятий онтологии идентификации нарушителя представлен в таблице 1. Онтологии позволяют структурировать знания при идентификации нарушителя, а также обеспечить формальное представление системы понятий ПрО и поддержку требуемой функциональности.

Таблица 1 – Фрагмент спецификации понятий онтологии процесса идентификации нарушителя

Понятия	Атрибуты	Отношения с атрибутами
Охрана	ФИО. Серия и номер удостоверения	Решение. СКБ
Вектор признаков	Имя. Номер. Дополнительная информация	Идентификация
Лицо	Положение губ. Положение бровей. Положение глаз	Биометрический признак
Походка	Размер шага. Темп. Вид	Биометрический признак. Движение тела

2 Классификация биометрических признаков при идентификации

Существует множество определений понятия и типологии нарушителя [4-6]. В работе под потенциальным нарушителем понимается человек, который совершает или может со-

вершить преступление, направленное на устрашение и насилие, добивается своих целей путём захвата заложников с угрозой их уничтожения (террорист). Для выработки эффективных мер, направленных на предотвращение преступлений террористического характера, необходимо иметь представление о личности потенциального нарушителя, что невозможно без изучения её особенностей (структуры, биометрических признаков, психологического портрета и др.) [7-10].

Признаки человеческого тела, поведенческие (походка, голос и др.), либо физиологические (лицо, отпечаток пальца, ДНК и др.) могут быть использованы в качестве биометрических признаков для распознавания личности. Данные признаки должны удовлетворять следующим свойствам: уникальность, универсальность (биометрические данные могут быть получены у любого человека независимо от их пола, возраста, местоположения), постоянство (например, рукописная подпись лица, выполненная в документе, должна визуально соответствовать подписи этого лица, содержащейся в иных документах), неуязвимость, собираемость [11].

В литературе рассматривается большое количество психологических портретов террористов. Личность нарушителя, совершившего преступление террористического характера, отличается от других категорий преступников (убийцы, воры, наркоманы и др.), во-первых, устойчивыми психологическими и психическими нарушениями, нарушениями социальной адаптации; во-вторых, преступлениями против человечества больше, чем против отдельных лиц (обычные преступники делают это больше для собственной выгоды) [12].

Деятельность террористов сложно распознать. Основными признаками поведения террориста являются: отрешённый взгляд, отсутствие визуального контакта с окружающими (жёсткий и сфокусированный взгляд вперёд), подчинённая поза, тяжёлая и скованная походка, определённая заторможенность реакций, внешне имеет вид собранного и умиротворенного человека [13-15]. Возможен и другой вариант их поведения, например, когда террорист может быть заметно возбуждён, агрессивен. Тогда у него может проявляться обильное выделение пота; он резко двигается, постоянно оглядывается, боясь слежки [14].

В работах [16-18] описаны основные черты лица террориста: неестественная бледность; скованное, каменное лицо, которое не выражает никаких эмоций; крупные и блестящие глаза; губы могут быть сильно сжаты либо чуть заметно двигаться (возможно чтение молитвы); возможные шрамы; и многие др.

Составить и выделить универсальный тип террориста невозможно, а можно лишь условно выделить некоторые биометрические признаки, характеризующие его [12, 13]. Сложность задачи обусловлена многоаспектностью такого явления как терроризм, а также многогранностью личности человека.

Основные типы биометрических признаков для выявления потенциального нарушителя изображены на рисунке 2 (адаптирован по материалам [19-21]).

Рисунок 2 – Типы биометрических признаков для выявления потенциального нарушителя

Физиологическими признаками для криминологии, сотрудников полиции и охраны являются движение тела и лицо [22, 23].

Физиологические (статические) биометрические признаки – признаки, присутствующие с рождением человека. Их получают в результате измерения части человеческого тела. Достоинства данных признаков в относительно ограниченной возможности их изменить и быстроте процесса распознавания с использованием компьютеров. Недостатки физиологических признаков: дороговизна биометрических сканеров; возможность повреждения биометрических идентификаторов; использование лицевых аксессуаров (кепки, очки, платки, маски и т.п.); необходимость определённых условий окружающей среды (освещение и т.п.).

Поведенческие (динамические) биометрические признаки – признаки, основанные на определенном шаблоне поведения (действия), выполняемого человеком (косвенно измеряют признаки облика человека). Главной особенностью данных признаков является использование времени в качестве метрики. Достоинствами поведенческих признаков являются: присутствие индивидуального набора анализируемых признаков; повышение точности распознавания в СКБ многофакторной идентификации. Недостатками являются: отсутствие метода и модели для оценки точности распознавания человека по движению тела; необходимость большого количества личных данных для верного определения поведения нарушителя, поскольку оно может меняться (усталость, опьянение, плохое самочувствие и т.п.).

Биометрические признаки имеют следующие общие достоинства: уникальные особенности для каждого человека; неизменные черты с течением времени [24]. Существуют ограничения, к которым биометрия уязвима, например, компьютерные атаки, изменение БД [25, 26].

Выявление потенциального нарушителя осуществляется в условиях множества биометрических признаков. Предлагается следующая классификация основных биометрических признаков, характеризующих потенциального нарушителя (рисунок 3, адаптирован по материалам [23, 27-29]).

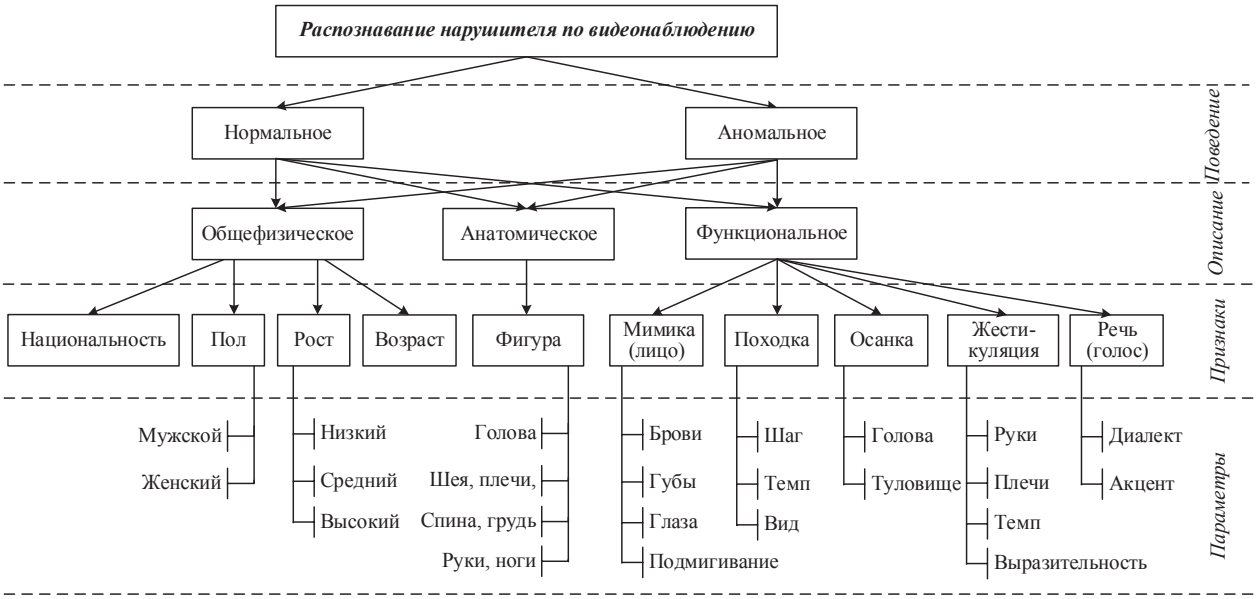

Рисунок 3 – Классификация основных биометрических признаков, характеризующих потенциального нарушителя

Поведение человека может быть «нормальным» и «аномальным (девиантным)». В настоящей работе под аномальным поведением понимается последовательность действий человека, которые не соответствуют модели типичного поведения в конкретной ситуации, имеют отклонение от нормы поведения, склонность к нарушениям, агрессии [28-30].

Описание внешности человека. Общефизическое описание – элементы внешности; анатомическое – описание всей фигуры в целом либо отдельных областей тела; функциональное – особенности, которые проявляются в движении. Каждый из анатомических признаков характеризуется по форме, размеру, положению, цвету [29]. При этом некоторые параметры могут быть представлены в виде словесного (нечёткого) описания, например, телосложение – слабое, очень слабое, среднее, коренастое, атлетическое; упитанность человека – худой, худощавый, средней упитанности, полный. Функциональное описание: мимика – движение мышц и элементов лица, которые могут меняться в зависимости от эмоционального состояния человека; походка – совокупность индивидуальных телодвижений при ходьбе; жестикуляция – комплекс движений рук, плеч, головы человека, которыми он сопровождает свою речь; речь – данные речевого механизма.

3 Виды систем распознавания

В настоящее время системы распознавания человека подразделяются на несколько видов (рисунок 4, адаптирован по материалам [24, 31-33]).

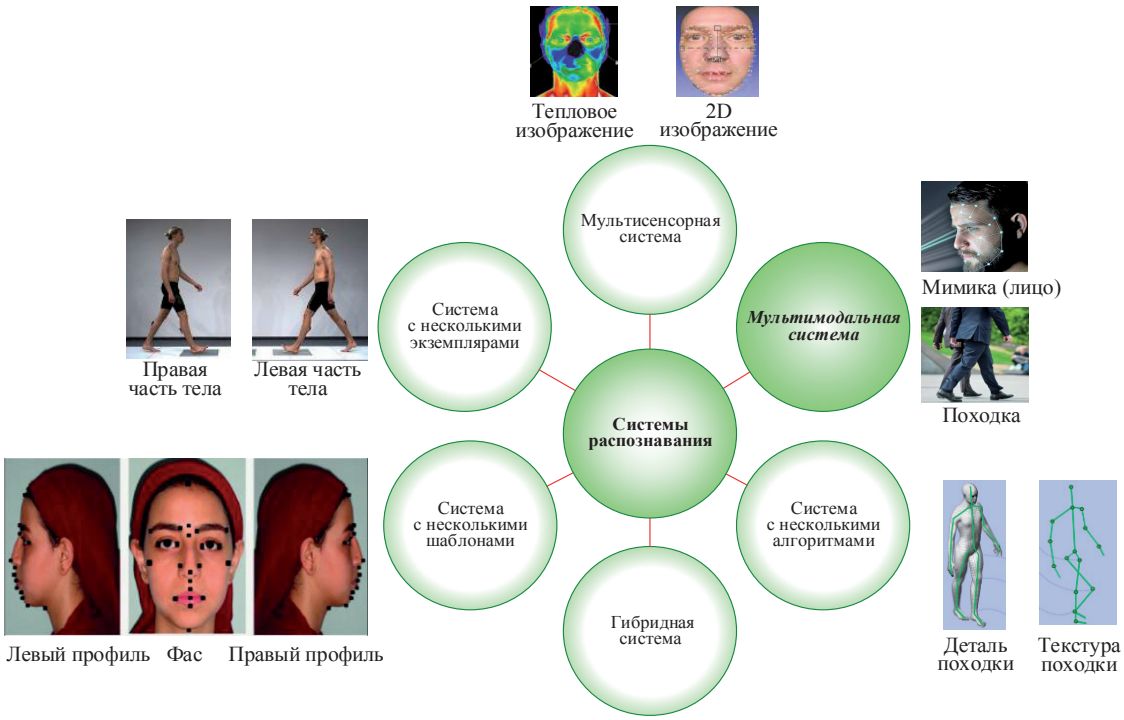

Рисунок 4 – Виды систем распознавания человека

Мультисенсорная система позволяет объединять полученные данные с различных датчиков (сканеров) для одного и того же биометрического признака для извлечения разнообразной информации (несколько датчиков – один биометрический признак). Например, данная система может использовать 2*D*, 3*D* или тепловое изображение лица для распознавания.

Мультимодальная система позволяет объединять более одного биометрического признака, что повышает точность распознавания человека. Например, данная система может использовать одновременно лицо и голос для распознавания человека. Такие системы являются дорогостоящими, поскольку для их работы требуется несколько датчиков, каждый из которых воспринимает различные биометрические признаки.

Система с несколькими алгоритмами позволяет обрабатывать один биометрический признак, полученный с одного датчика с использованием различных подходов к извлечению признаков и различных алгоритмов сопоставления (несколько алгоритмов – один биометрический признак). Например, система распознавания отпечатков пальцев, походки может использовать как детали, так и особенности текстуры для сопоставления отпечатков пальцев и походки.

Гибридная система позволяет объединять более одной из вышеупомянутых биометрических систем для надёжного распознавания. Например, если два алгоритма распознавания лица будут объединены с двумя алгоритмами распознавания отпечатков пальцев, то такая система будет мультимодальной с несколькими алгоритмами.

Система с несколькими шаблонами позволяет использовать несколько шаблонов одного и того же биометрического признака, полученных с помощью одного датчика (несколько образцов с одним датчиком – один биометрический признак). Например, при распознавании человека по снимкам лица, которые сделаны при разных точках доступа и освещении.

Система с несколькими экземплярами позволяет фиксировать несколько экземпляров одного и того же биометрического признака (несколько экземпляров – один биометрический признак). Например, изображения левой и правой частей тела, отпечатки двух или более пальцев или ладоней человека могут быть объединены по одному изображению одного и того же человека.

При распознавании человека встречаются *унимодальные системы*, позволяющие использовать один биометрический признак человека для распознавания и проверки. Данные системы предлагают надёжное решение для приложений идентификации и верификации, однако необходимо учитывать ограничения их использования, которые могут привести к ошибкам распознавания.

- Шумы в измеряемых данных (изображение отпечатка пальца со шрамом; образец голоса, изменённый холодом; плохая освещённость лица и др.).
- Неуниверсальность – отсутствие получения значимых биометрических данных (система распознавания радужной оболочки не может получить информацию потенциального нарушителя с длинными ресницами, опущенными веками, патологией глаз).
- Поддельные атаки, которые встречаются при использовании поведенческих признаков (подпись, голос, походка и др.). В этом случае система, основанная только на анализе одного признака, может привести к неверному распознаванию. Если система включает дополнительный признак, то это приведёт к увеличению вероятности распознавания (маловероятно, что у двух разных людей одинаковая походка и лицо).

При распознавании человека СКБ, основанные на слиянии многих биометрических признаков, способны эффективно обрабатывать зашумлённые или некачественные данные (характерно для систем, основанных на распознавании лица и голоса) [33].

Интеграция разнородной информации, поступающей из разных источников, является одним из основных приёмов проектирования СКБ по распознаванию человека, основанных на слиянии множества биометрических признаков [33-36].

СКБ должны соответствовать следующим критериям [31, 32, 37-39].

- *Универсальность* – каждый нарушитель обладает своими уникальными биологическими признаками. Люди без рук, пальцев, с нарушением походки, осанки или с повреждёнными глазами также должны быть зарегистрированы и учтены.
- *Уникальность, отличительность* – никакие два любых нарушителя не могут быть одинаковыми с точки зрения биометрических признаков. Уникальность может измеряться частотой ложного сопоставления.
- *Надёжность* – биометрические признаки должны быть неизменными в течение определённого периода времени. Радужная оболочка глаза обычно остаётся неизменной на протяжении десятилетий, лицо человека со временем значительно меняется, палец часто подвергается травмам, подпись и её динамика также может измениться. Надежность может измеряться частотой ложных несоответствий.
- *Представление* – достижение точности и скорости распознавания с учетом задействованных эксплуатационных факторов и факторов окружающей среды, необходимых для достижения приемлемой точности.
- *Приемлемость* – у пользователей и общественности не должно быть возражений против измерения/сбора биометрических признаков.
- *Доступность, собираемость* – биометрический признак может быть измерен количественно с помощью какого-либо сенсорного устройства и легко визуализирован. Доступность может быть количественно оценена по пропускной способности системы.
- *Устойчивость к обходу* – тесты и доказательства того, что разработанная система противостоит мошенническим методам.

Сравнение биометрических признаков для выявления потенциального нарушителя с использованием рассмотренных критериев СКБ представлено в таблице 2, адаптированной по материалам [32, 38].

Таблица 2 – Сравнение биометрических признаков

Критерии СКБ / Биометрические признаки	Универсальность	Уникальность	Надёжность	Доступность	Представление	Приемлемость	Устойчивость к обходу
Мимика (лицо)	высокая	низкая	средняя	высокая	низкое	высокая	средняя
Походка	высокая	низкая	средняя	высокая	низкое	высокая	высокая
Жестикуляция	средняя	низкая	средняя	средняя	низкое	высокая	средняя
Осанка	средняя	низкая	низкая	средняя	низкое	высокая	средняя

Какой биометрический признак является наилучшим, однозначно ответить нельзя, поскольку каждый признак имеет свои сильные и слабые стороны, и выбор обычно зависит от постановки задачи.

4 Слияние биометрических данных

Схема слияния биометрических данных и распознавания нарушителя по движениям тела и лицу, которая может лежать в основе разработки СКБ, представлена на рисунке 5.

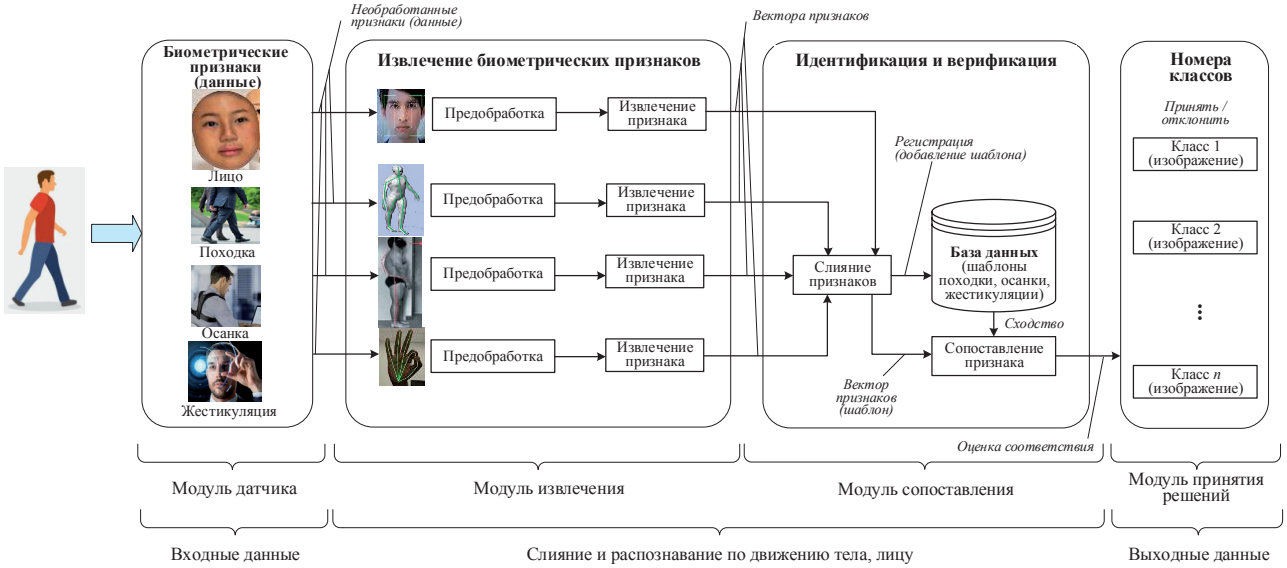

Рисунок 5 – Структурная схема слияния биометрических данных и распознавания нарушителя по движениям тела и лицу

СКБ, работающие с множеством биометрических признаков, состоят из модулей [31, 40, 41]:

- *модуль датчика* собирает биометрические данные человека (например, датчик отпечатков пальцев), которые задаются в качестве входных данных и служат входом для модуля извлечения признаков;
- *модуль извлечения (выделения) признаков* извлекает значения признаков после предобработки (например, положение и ориентация мелких точек на изображении отпечатка пальца), которые дают компактное представление этих признаков;
- *модуль сопоставления (соответствия)* сравнивает значения признаков со значениями в шаблоне, которые хранятся в БД, путём создания соответствующей оценки (степень сходства или расхождения между двумя биометрическими векторами признаков), которая передаётся в модуль принятия решений;

- *модуль принятия решений* устанавливает (выявляет) нарушителя, который либо подтверждается, либо отклоняется на основе оценки соответствия, сгенерированной в модуле сопоставления, либо распознаёт личность человека.

Важный вопрос, возникающий при слиянии биометрических признаков, - определение типа данных, которые должны быть объединены и выбор метода слияния [31]. Классификация уровней слияния в СКБ, работающих с множеством биометрических данных, которые могут быть объединены на различных уровнях показана на рисунок 6 (адаптирован по материалам [31, 40-42]).

Рисунок 6 – Классификация уровней слияния в СКБ

Согласно категории *до сопоставления признаков* слияние осуществляется на уровне датчиков, на уровне признаков до того, как будет выполнено сопоставление биометрических данных [37, 38, 40-43].

Слияние на уровне датчиков – объединение необработанных данных, полученных с различных биометрических датчиков, в один вектор. Информация одного и того же биометрического признака, полученного с различных датчиков, объединяется для получения единого биометрического признака. Т.е. дополнительная информация, соответствующая, например, отпечаткам пальцев, которая может быть получена с использованием различных типов датчиков, интегрируется с использованием метода слияния на уровне датчиков. Другой пример – изображения лиц, полученные с нескольких камер, могут быть объединены для формирования единого изображения лица.

Структура *слияния на уровне датчиков* представлена на рисунке 7. Данные поступают с разных датчиков, которые должны быть совместимы, что не всегда возможно (например, может оказаться невозможным объединить изображения лиц, полученные с камер с разным разрешением); все методы должны быть совместимы с исходными данными и известны заранее [44]; один датчик или различные совместимые датчики (отпечаток пальца, сканер радужной оболочки глаза и т.д.) представляют шаблоны (образцы) одного обнаруженного биометрического признака. Данное слияние рекомендуется для систем с множеством датчиков и несколькими выборками, которые делают несколько снимков одной и той же биометрической информации [45]. Предполагается, что это повысит точность распознавания.

Слияние на уровне признаков – слияние векторов признаков, которые получены либо с использованием нескольких датчиков, либо с использованием нескольких алгоритмов извле-

чения признаков из одних и тех же датчиков (векторы признаков одного биометрического признака, полученные от разных датчиков; векторы признаков одного биометрического признака, полученные от разных объектов (векторы признаков отпечатков пальцев левой и правой руки); векторы признаков, сгенерированные из нескольких биометрических признаков) (рисунок 8).

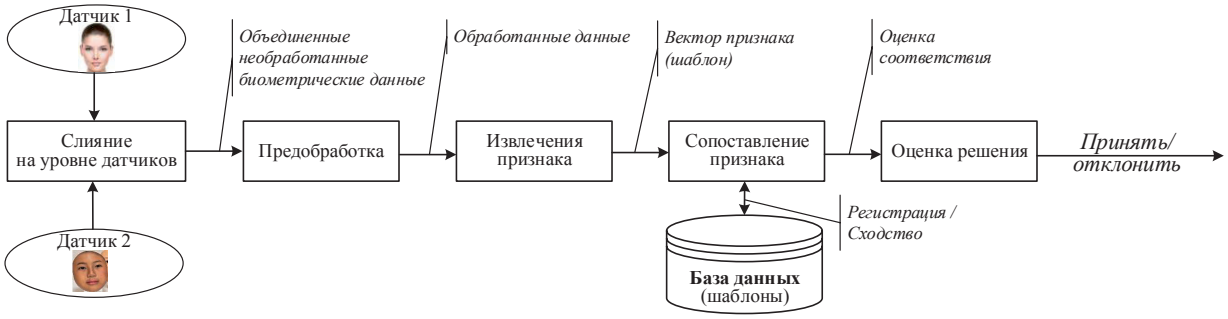

Рисунок 7 – Слияние данных на уровне датчиков

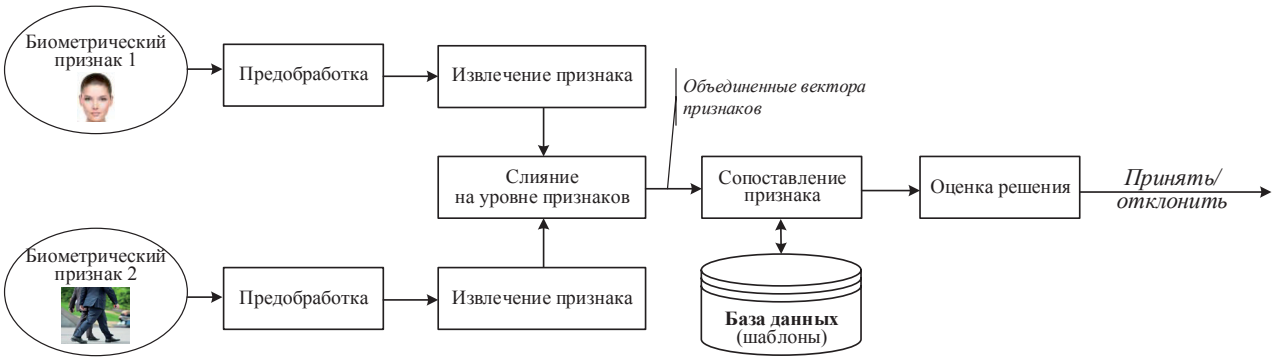

Рисунок 8 – Слияние данных на уровне признаков

Если признаки, извлечённые из одного биометрического признака, не зависят от признаков, извлечённых из другого, можно объединить два вектора в один новый вектор, который может быть как однородным, так и гетерогенным. Когда векторы признаков однородны (например, множественные отпечатки пальцев нарушителя), один результирующий вектор признаков может быть вычислен как средневзвешенное значение отдельных векторов. Когда векторы признаков неоднородны (например, векторы признаков, полученные с использованием различных методов извлечения признаков, или векторы признаков различных биометрических признаков), то происходит объединение с целью формирования единого вектора признаков. Объединение невозможно, когда наборы признаков несовместимы (например, признаки пальцев и лица). Новый вектор признаков имеет более высокую размерность и представляет личность человека в подробном виде, который сравнивается с шаблоном регистрации (объединённым вектором признаков, хранящимся в БД).

При слиянии векторов признаков необходимо учитывать трудности, возникающие по следующим причинам [37, 40]:

- объединение двух векторов признаков может привести к получению вектора признаков с очень большой размерностью;
- большая размерность вектора признаков приводит к увеличению вычислительных ресурсов и ресурсов хранения;
- большинство коммерческих биометрических систем не предоставляют доступ к векторам признаков, которые они используют в своих продуктах.

Сдерживающим фактором при распознавании нарушителя является отсутствие единой общедоступной БД биометрических образцов преступников.

Согласно категории *после сопоставления признаков* слияние осуществляется на уровнях оценки сопоставления, ранга и принятия решений (см. рисунок 6) [32, 40, 45].

Слияние на уровне оценки сопоставления (*достоверности*) – векторы признаков, создаваемые независимо для каждого датчика, сравниваются с шаблонами, которые хранятся в БД отдельно для каждого биометрического признака, и объединяются для оценки соответствия в виде одиночного скалярного балла (показателя). Данные оценки могут быть объединены для подтверждения подлинности заявленной личности. Структура слияния на уровне оценки сопоставления представлена на рисунке 9.

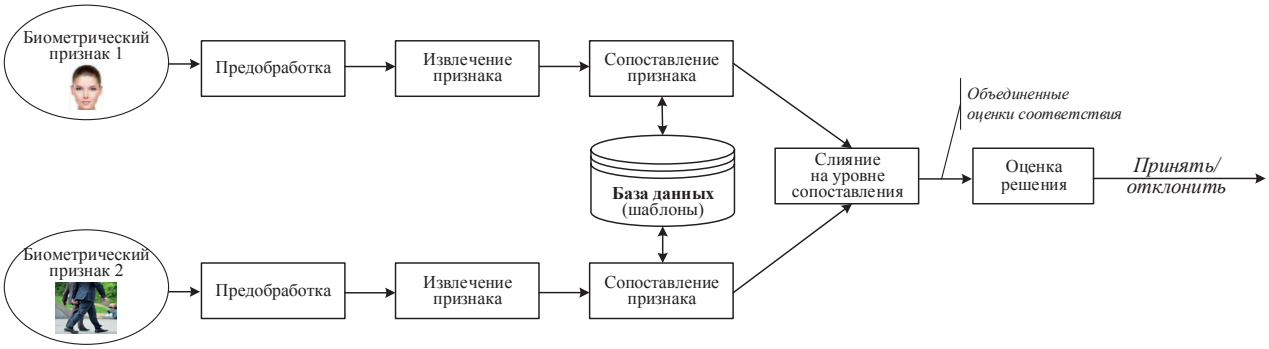

Рисунок 9 – Слияние данных на уровне оценки сопоставления

Соответствующий балл указывает на близость входного вектора признаков к вектору шаблона. Совпадающие баллы не могут напрямую быть использованы или объединены, поскольку оценки получены из разных датчиков и основаны на разных методах масштабирования. Для решения данной задачи введены три варианта схемы слияния: на основе плотности, преобразования, классификатора [46, 47].

Схема на основе плотности основана на оценке распределения баллов. Данная схема включает фильтр Калмана, расширенный фильтр Калмана и методы слияния фильтров частиц. Схема обеспечивает точную оценку, но требует большого количества тренировочных образцов, а также больше времени и усилий для настройки работы по сравнению с другими схемами.

Схема на основе преобразования обычно применяется для нормализации баллов. Этот процесс необходим для изменения масштаба параметров с целью обеспечения совместимости между несколькими переменными оценки [48]. Эта схема может быть применена с использованием различных методов (правило суммы, правило произведения, минимальное правило и максимальное правило).

В схеме на основе классификатора оценки соответствия, полученные с помощью нескольких сопоставителей, объединяются для построения единого вектора признаков, который затем передаётся в подходящий классификатор с целью получения заключительной метки: является ли пользователь законным или самозванцем. Для классификации вектора соответствия в этой схеме применяются: метод опорных векторов, байесовский вывод, теория Демпстера-Шефера, модель максимальной энтропии, нейронная сеть.

Слияние на уровне ранга – объединение рангов, полученных каждым отдельным биометрическим сопоставлением, и определение нового ранга, который будет использоваться при принятии окончательного решения. Высокий ранг указывает на хорошее соответствие. Слияние на уровне ранга используется для идентификации, а не для верификации [49].

Слияние на уровне принятия решений – формирование окончательного решения из полученных индивидуально отдельных решений о личности нарушителя по различным биомет-

рическим признакам (рисунок 10) с использованием различных методов, например, метода голосования большинством.

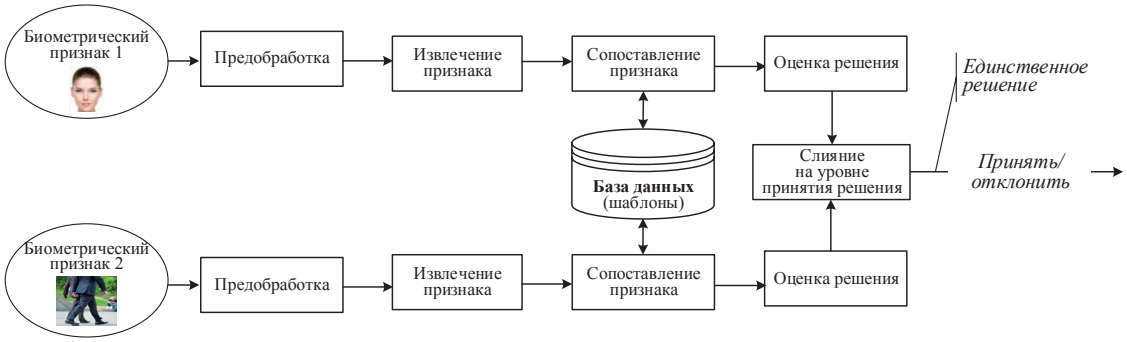

Рисунок 10 – Слияние данных на уровне принятия решения

Главное преимущество метода голосования большинством заключается в том, что он не требует предварительных знаний о сопоставителе, а также подготовки для принятия окончательного решения.

СКБ могут работать либо в режиме верификации, либо в режиме идентификации (см. рисунок 5). Процесс биометрической аутентификации (процесс проверки подлинности личности) разделен на три основных этапа (рисунок 11 адаптирован по материалам [37, 38]).

Регистрация – процесс регистрации нового человека в системе. На данном шаге сначала биометрический признак личности фиксируется датчиком для генерирования цифрового представления признака. Датчик должен получать всю важную информацию о личности, которая обычно представлена в виде изображения. Затем осуществляется предварительная обработка биометрических данных X (улучшение, нормализация, сегментация и удаление шума). Целью нормализации элемента является изменение местоположения (среднего) и масштаба (дисперсии) значения элемента с помощью функции преобразования, чтобы отобразить их в общую область. Далее происходит извлечение набора признаков из обработанных биометрических данных X' для создания эталонного шаблона Z_X. Этот шаг является решающим, поскольку для успешного распознавания потенциального нарушителя необходимо извлечь и выбрать правильные признаки. Шаблон Z_X, представляющий личность потенциального нарушителя, который будет использоваться для последующего сравнения, сохраняется в БД. Как видно из рисунка 5 этап регистрация является общим, как для этапа верификации, так и для этапа идентификации.

Верификация – процесс проверки подлинности личности потенциального нарушителя путём сравнения (1:1 соответствие) предоставленной биометрическим признаком Z_Q (биометрический признак запроса, полученный на этапах распознавания) с хранимым в БД шаблоном, который соответствуют заявленному нарушителю Z_X. Т.е. необходимо определить, является ли заявленная личность действительной? (является ли этот человек тем, за кого он себя выдаёт?). Результирующая оценка соответствия S (балл) сравнивается с сохранённым пороговым значением, вычисленным для заявленного потенциального нарушителя, или общим пороговым значением. Оценка соответствия определяется в диапазоне от 0 до 100 %.

Идентификация – процесс распознавания личности потенциального нарушителя путём сравнения биометрического признака Z_Q со всей БД ($Z_X=\{X_1, X_2,\ldots, X_m\}$, где m – количество нарушителей, зарегистрированных в БД) путём «один ко многим», (1:N) с заданной степенью сходства. Т.е. требуется ответить на вопрос: «Кто этот человек?». Далее неизвестному лицу может быть присвоен идентификатор, соответствующий наиболее похожему профилю, найденному в БД, либо отклоняется это лицо. Если совпадение не найдено, это означает, что данное лицо не зарегистрировано в БД. Решение о принятии или отклонении человека принимается путём сравнения ответа системы с пороговым значением (называемым порогом принятия решения). В результате будет выбрана наиболее похожая личность по используемой геометрии лица искомого человека, а не идентичная, как в процессе верификации. В этом случае будет идентификация или ответ, что данное лицо есть в БД. Если лицо отсутствует в БД, или степень сходства является меньше заданной для всех сравнений, то результата не будет. Ошибка системы возрастает за счёт сравнения «один ко многим», и этап идентификации становится критическим для системы распознавания.

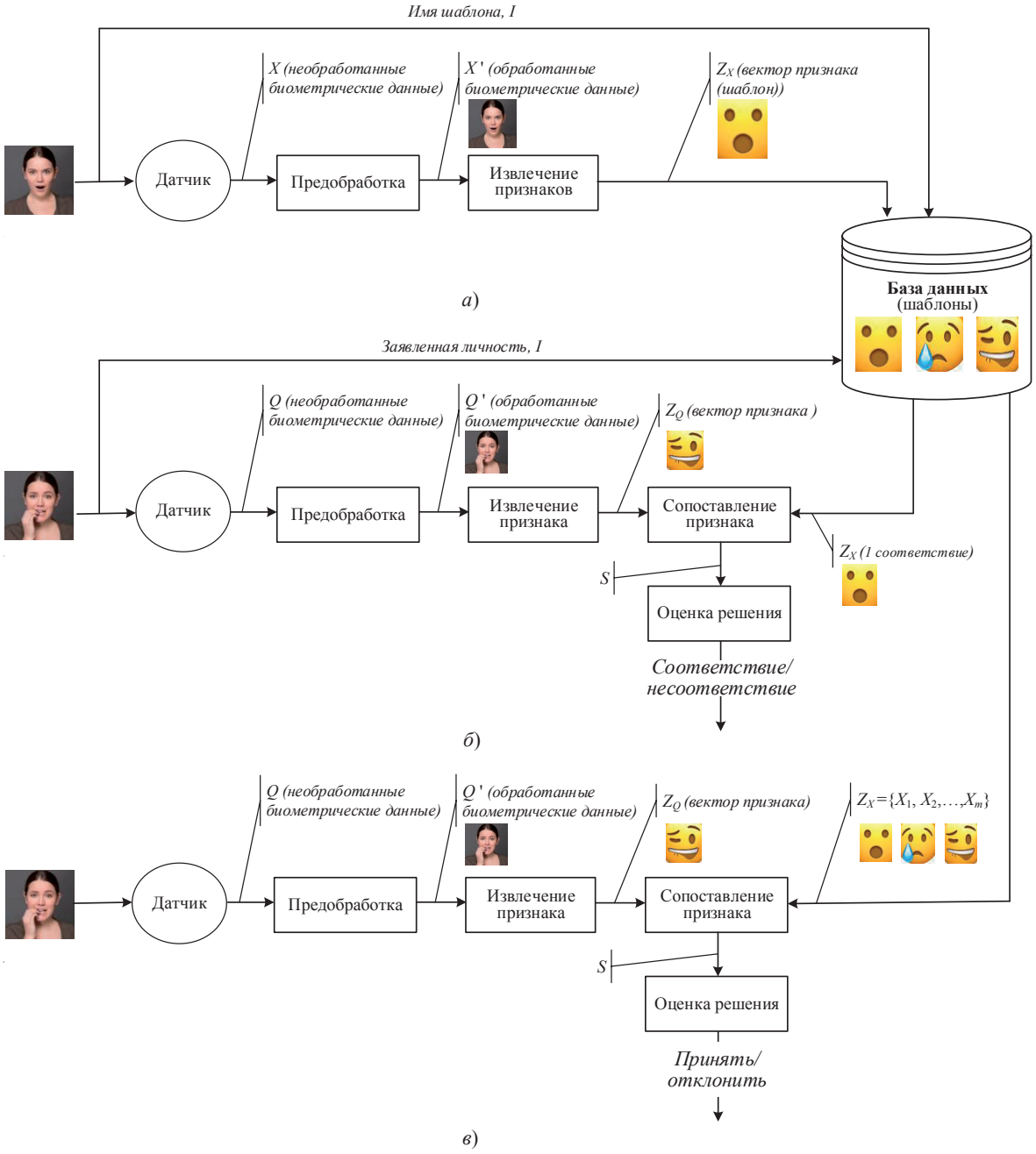

Рисунок 11 – Схемы процесса биометрической аутентификации:
а) этап регистрации; б) этап верификации; в) этап идентификации
X – признак, полученный во время регистрации; Z_X – набор признаков шаблона; Z_Q – набор признаков запроса; Q – биометрический признак запроса (выборка), полученный на этапах распознавания; S – оценка соответствия; M – количество нарушителей, зарегистрированных в БД

5 Методы и технологии распознавания человека по движению тела и лицу

Для решения задачи распознавания личности на видео по движению тела и лицу разработано большое количество различных методов. Классификация методов и технологий, которые используются при распознавании человека по движениям тела и лицу в видеонаблюдениях, показана на рисунке 12 (адаптирован по материалам [50-59]).

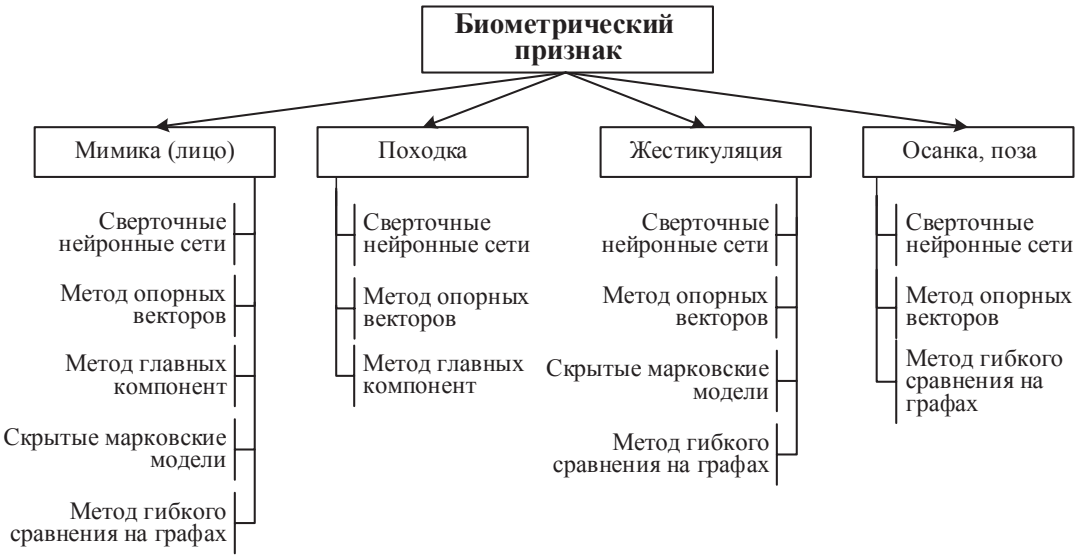

Рисунок 12 – Классификация методов и технологий распознавания человека по движению тела и лицу

Приведённое разделение методов и технологий, применяющихся при распознавании личности, носит условный характер, поскольку на практике они пересекаются и взаимодействуют между собой. В этом случае применяются гибридные подходы, сочетающие в себе различные методы и технологии распознавания человека. Ключевым моментом при их разработке является то, что они не должны конфликтовать между собой.

Наиболее применяемыми являются следующие методы:

Свёрточные нейронные сети (*Convolutional Neural Networks*, *CNN*) – это класс искусственных нейронных сетей, чаще всего применяемых для задач классификации, обнаружения и анализа объектов на изображении, сконцентрированных на небольших участках изображения, и выделении в них важных особенностей. В работе [50] представлена модифицированная архитектура *CNN* для извлечения отличительных черт лица путём добавления двух операций нормализации к двум слоям. Операция нормализации представляет собой пакетную нормализацию, которая обеспечивает ускорение работы *CNN*. Для классификации лиц использовался классификатор *Softmax*.

В работе [51] предложен подход, основанный на идее многоклассовой классификации на видеопоследовательностях. Оценка качества предлагаемого подхода проводилась на основе набора данных, который включает более 15000 видеопоследовательностей. В качестве классификаторов были апробированы пять архитектур нейронных сетей. Результаты исследований показали, что предлагаемый подход может осуществлять идентификацию человека в режиме реального времени без использования специализированного оборудования с точностью около 80 %.

В работе [52] предложена новая модель *CNN* для распознавания походки на основе позы. Данная модель учитывает движение точек в областях вокруг суставов человека. Для извлечения информации о движении оценивается оптический поток между последовательными кадрами.

Метод опорных векторов (*Support Vector Machines, SVM*) – один из самых известных алгоритмов обучения с учителем, применяемый для задачи классификации и регрессии в машинном обучении. В работе [53] предложен метод распознавания лиц на основе комбинирования анализа основных компонентов ядра (*Kernel Principal Component Analysis*, *KPCA*) и метода опорных векторов. Сначала используется метод *KPCA* для извлечения признаков из входных изображений, а затем применяется метод *SVM* к извлечённым признакам для классификации входных изображений.

В работе [54] описан прототип системы реального времени, способной распознавать четыре жеста, которые соотносятся с человеческими эмоциями на основе движений рук. Предложена структура для использования датчика походки *Kinect* для идентификации жеста. Объекты, извлечённые из 3*D*-скелета с помощью датчика *Kinect v*2, классифицируются с использованием метода *SVM*.

В работе [55] предложен метод распознавания поз человека с использованием классификатора *SVM*. Для одновременной съёмки двух наборов последовательностей изображений используются две камеры. После захвата последовательностей изображений используется алгоритм сегментации движущихся объектов, чтобы от-

личить человеческое тело от фона. Экспериментальные результаты показали, что предложенный метод обеспечивает высокую скорость и уровень распознавания.

Недостатками метода опорных векторов являются существенные временные затраты при настройке и необходимость большого объема памяти.

Метод главных компонент (*Principal Components Method, PCA*) обеспечивает уменьшение размерности пространства биологических признаков с наименьшими потерями информации. Например, в работе [56] рассмотрены некоторые аспекты применения метода главных компонент для решения задачи распознавания изображений. Предложен алгоритм многоуровневой линейной конденсации для вычисления главных компонент больших наборов изображений. Данный алгоритм использует аппроксимацию, которая позволяет сократить порядок матриц с сохранением собственных значений в заданном диапазоне.

В работе [57] предлагается метод распознавания личности по походке, регистрируемой с использованием видеосъемки в оптическом диапазоне, состоящий в выделении движущегося человека на видеоряде с последующей нормализацией размера и снижением размерности с использованием метода главных компонент и классификацией с использованием метода опорных векторов. Экспериментальные исследования показали высокую точность распознавания личности (не менее 90 %).

Недостатками метода главных компонент являются: потеря некоторой информации, стандартизация данных по единичной шкале; ковариационную матрицу трудно оценить точным образом, даже простейшая инвариантность не может быть зафиксирована *PCA* [58], чувствительность к входным данным.

Скрытые марковские модели (*Hidden Markov Models, HMM*) учитывают пространственно-временные характеристики сигналов, поэтому получили широкое применение в распознавании изображений лиц. Например, в работе [59] предлагается метод распознавания лиц на основе скрытой марковской модели. Предложенный метод снижает вычислительную сложность распознавания лиц на основе *HMM*, при этом немного повышая скорость распознавания.

Недостатками *HMM* являются: ограниченные применения при не очень большом объёме БД; необходимость подбирать параметры модели для каждой конкретной БД.

Метод гибкого сравнения на графах (*Elastic Bunch Graph Matching*) – метод компьютерного зрения для распознавания объектов или классов объектов в изображении на основе графического представления, извлечённого из других изображений. Данный метод использовался для распознавания и анализа лиц, а также для жестов и других классов объектов.

Недостатками метода гибкого сравнения на графах являются: вычислительная сложность процесса распознавания, а также низкая технологичность при запоминании новых эталонов.

Заключение

Распознавание человека по движениям тела и лицу в видеонаблюдениях играет важную роль в обеспечении безопасности на объектах с массовым скоплением людей, т.к. позволяет раскрыть личность потенциального нарушителя, совершающего преступления, а также предупредить преступления.

Рассмотрены структурные схемы слияния биометрических признаков и принципы их работы, приведено сравнение методов и технологий распознавания человека по движению тела и лицу, показаны их достоинства и недостатки.

На основании проведённого анализа могут быть сформулированы общие рекомендации для разработчиков СКБ по видеонаблюдению:

- СКБ необходимо проектировать как систему поддержки принятия решений;
- необходимо разработать базовую архитектуру СКБ и процесс аутентификации по движению тела и лицу (при комбинировании технологически отработанных методов);
- информационной основой проектируемой СКБ должны быть значения различных биометрических признаков;
- рекомендуется применять мультимодальные системы, которые позволяют объединять несколько биометрических признаков;
- необходимо определить, как будет осуществляться распознавание нарушителя - по одному или по нескольким признакам, как они получены (с одного или нескольких датчиков), и выбрать уровень слияния биометрических признаков.

Список источников

[1] Состояние преступности в России за январь - ноябрь 2022 года. Москва. Генеральная прокуратура Российской Федерации. 60 с. http://crimestat.ru/analytics.

[2] Типовая модель действий нарушителя, совершающего на объекте образования преступление террористической направленности в формах вооруженного нападения, размещения взрывного устройства, захвата заложников, 41 с. https://minobrnauki.gov.ru.

[3] ***Зенов А.Ю.*** Комплексный подход к обнаружению, классификации и распознаванию нарушителя на охраняемой территории // *Известия высших учебных заведений. Поволжский регион. Технические науки*. 2012. № 2 (22). С.23-32.

[4] ***Смирнов А.М.*** К вопросу о фундаментально-теоретической модели изучения личности преступника // *Гуманитарные, социально-экономические и общественные науки*. 2020. № 1. С.1-5. DOI: 10.23672/SAE.2020.1.53256.

[5] ***Ким Е.В., Ри П.Г.*** Личность преступника: криминологический анализ // *Ученые заметки ТОГУ*. 2013. Т.4. № 4. С.402-407.

[6] ***Абельцев С.Н.*** О личности преступника и практической значимости ее изучения // *Вестник Тамбовского университета. Гуманитарные науки*. 2000. № 3 (19). С.83-85.

[7] ***Копылова Г.К., Прозоров А.В.*** Психология в деятельности органов внутренних дел. М.: ЦОКР МВД России, 2006. 236 с.

[8] ***Герасименко В.А.*** Основы защиты информации в АС. М.: Наука, 2001. 178 с.

[9] ***Ольшанский Д.В.*** Психология терроризма. М.: Юрайт, 2015. 194 с.

[10] ***Стуколова Л.С., Закирова Д.А.*** Психология современного терроризма // *Аллея науки*. 2018. Т.5. № 6 (22). С.546-549.

[11] ***Jain, A.K., Ross A., Prabhakar S.*** An introduction to biometric recognition // *IEEE Trans. Circuits Syst. Video Technol*. 2004. Vol.14. No.1. P.4-20. DOI: 10.1109/TCSVT.2003.818349.

[12] ***Газизулин А.И.*** Криминологическая характеристика личности террориста нашего времени // *NovaInfo.Ru*. 2018. Т.1. № 84. С.161-165. DOI: 10.24411/2312-0444-2021-4-292-297.

[13] ***Аренова Л.К., Набиева Е.А.*** Личность лица, совершившего акт терроризма // *Актуальные проблемы права и государства в XXI веке*. 2018. Т. 10. № 1. С.38-46.

[14] ***Пимакова О.Г.*** Личность преступника террориста // *Виктимология*. 2018. № 4 (18). С. 54-58.

[15] ***Тарчоков Б.А.*** Мотивационные особенности вовлечения молодежи в террористическую деятельность // *Историческая и социально-образовательная мысль*. 2015. № 6. С.211-213. DOI: 10.17748/2075-9908-2015-7-6/1-211-213.

[16] ***Шендра С.Е., Хонин А.А., Войлошников А.Д.*** Психологический портрет личности террориста // *Молодой ученый*. 2022. № 13.1 (408.1). С.32-33.

[17] ***Малеева М., Кленикова Е., Мартынова Я.*** Психологический портрет террориста, 7 с. https://scienceforum.ru/2017/article/2017038036.

[18] ***Лепешкин Н.Я., Василин В.Г., Обирин А.И., Талынев В.Е.*** Психологические основы терроризма и антитеррористической деятельности в современных условиях. Хабаровск: Хабаровский пограничный институт Федеральной службы безопасности Российской Федерации, 2008, 348 с.

[19] ***Bouchrika I., Jain S., Arora S., Singh U.P.*** A Survey of using biometrics for smart visual surveillance: gait recognition // Advanced Sciences and Technologies for Security Applications. 2018. P.3-23. DOI: 10.1007/978-3-319-68533-5_1.

[20] ***Singh J.P.*** Vision-based gait recognition: a survey // IEEE Access. 2018. Vol.6. P.70497-70527. DOI: 10.1109/ACCESS.2018.2879896.

[21] ***Priyanka S, Kaur M.*** Classification in pattern recognition: a review // IJARCSSE All Rights Reserved. 2013. Vol. 3. P.298-306.

[22] ***Кобец П.Н.*** О комплексном изучении личности преступника в отечественной криминологии // *Проблемы развития личности*: матер. международ. науч.-практ. конф. Прага, 2013. С.93-95.

[23] ***Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р.*** Криминалистика: учебник для вузов. М.: НОРМА (НОРМА–ИНФРА М), 2001. 908 с.

[24] ***Ryszard C.*** Multimodal biometrics for person authentication. 2020, 516 p. https://www.researchgate.net/publication/345480873_Multimodal_Biometrics_for_Person_Authentication. DOI: 10.5772/intechopen.85003.

[25] ***Evans N., Marcel S., Ross A., Teoh ABJ.*** Biometrics security and privacy protection //IEEE Signal Process Mag. 2015. Vol.32(5). P.17-18. DOI: 10.1109/MSP.2015.2443271.

[26] ***Anil K.Jain, Nandakumar Karthik, Ross Arun.*** 50 years of biometric research: Accomplishments, challenges, and opportunities // Pattern Recognition Letters. 2016. Vol.79. P.80-105. DOI:10.1016/j.patrec.2015.12.013.

[27] Криминалистическое исследование внешних признаков человека (габитоскопия). Физиогномика убийцы или как определить преступника по внешности: словесный портрет с полным описанием, 17.04.2021. https://lehre.ru/do/kriminalisticheskoe-issledovanie-vneshnih-priznakov-cheloveka-gabitoskopiya.html.

[28] ***Федюнина А.П.*** Выявление характерологических признаков и составление психологического портрета возможного нарушителя и лояльного сотрудника в сфере информационной безопасности // *Вестник АГТУ*. 2007. № 4. С. 231-236.

[29] Словесный портрет. Описание внешности человека по методу словесного портрета. 05.11.2021. https://goaravetisyan.ru/slovesnyi-portret-opisanie-vneshnosti-cheloveka-po-metodu-slovesnogo.

[30] ***Акимов А.А., Мустафина С.А.*** Обзор современных методов искусственного интеллекта по распознаванию девиантного поведения индивида // *Вестник Технологического университета*. 2020. Т. 23. № 8. С.69-79.

[31] ***Siddiqui A.M.N., Telgad R., Deshmukh P.D.*** Multimodal biometric systems: study to improve accuracy and performance // *International Journal of Current Engineering and Technology*. 2014. Vol.4. No.1. P.165-171.

[32] ***Gad R., Nawal El-Fishawy, Ayman El-Sayed, Zorkany M.*** Multi-biometric systems: a state of the art survey and research directions // International Journal of Advanced Computer Science and Applications. 2015. Vol. 6(6). P. 128-138. DOI:10.14569/IJACSA.2015.060618.

[33] ***Ayodele Oloyede, Aderonke Adegbenjo.*** Current practices in information fusion for multimodal biometrics // American Journal of Engineering Research (AJER). 2017. Vol. 6. P.148-154.

[34] ***Ковалев С.М., Колоденкова А.Е., Снасель В.*** Интеллектуальные технологии слияния данных при диагностировании технических объектов // *Онтология проектирования*. 2019. Т.9. №1(31). С.152-168. DOI: 10.18287/2223-9537-2019-9-1-152-168.

[35] ***Долгий А.И., Колоденкова А.Е., Ковалев С.М.*** Проблемы и методы слияния разнородных данных в гибридных интеллектуальных системах // *Гибридные и синергетические интеллектуальные системы*: матер. IV Всерос. Поспеловской конференции с междунар. участием. 2018. С.181-187.

[36] ***Ailon N., Charikar M., Newman A.*** Aggregating inconsistent information: ranking and clustering // In Proceedings of 37th Annual ACM Symposium on Theory of Computing (STOC). 2015. P.684-693.

[37] ***AlMahafzah H., AlRwashdeh M.Z.*** A Survey of multibiometric systems // International Journal of Computer Applications. 2012. Vol.43. No.15. P.36-43.

[38] ***Soltane M., Bakhti M.*** Multi-modal biometric authentications: concept issues and applications strategies // *International Journal of Advanced Science and Technology*. 2012. Vol. 48. P.1-38.

[39] ***Sathish G., Saravanan S.V., Narmadha S., Maheswari S.U.*** Multi-algorithmic iris recognition // International Journal of Computer Applications. 2012. Vol.38. No.11. P.13-21.

[40] ***Mwaura G.W., Mwangi W., Otieno C.*** Multimodal biometric system: fusion of face and fingerprint biometrics at match score fusion level. *International Journal of Scientific & Technology Research*. 2017. Vol. 6. P.41-49.

[41] ***Ross A., Jain A.*** Information fusion in biometrics. *Pattern Recognition Letters*. 2003. P.2115-2125.

[42] ***Delac K., Grgic M.*** A Survey of biometric recognition methods // 46th International Symposium, ELMAR-2004, 2004. P.184-193.

[43] ***Aly O.M., Salama G.I., Mahmoud T.A., Onsi H.M.*** A multimodal biometric recognition system using feature fusion based on PSO // International Journal of Advanced Research in Computer and Communication Engineering. 2013. Vol.2. P.4336-4343. DOI:10.1007/s10916-019-1391-5.

[44] ***Ghayoumi M.*** A review of multimodal biometric systems: fusion methods and their applications. IEEE/ACIS 14th International Conference Computer and Information Science (ICIS). 2015. P.131-136. DOI: 10.1109/ICIS.2015.7166582.

[45] ***Radha N.***, ***Kavitha A.*** Rank level fusion using fingerprint and iris biometrics // Indian Journal of Computer Science and Engineering (IJCSE). 2011. Vol.2. No.6. P.917-923.

[46] ***Haryati Jaafar, Dzati Athiar Ramli.*** A review of multibiometric system with fusion strategies and weighting factor // International Journal of Computer Science Engineering (IJCSE). 2013. Vol.2. No.4. P.158-165.

[47] ***Abderrahmane H., Noubeil G., Ziet L., Zahid A., Dipankar D.*** Weighted quasi-arithmetic mean based score level fusion for multi-biometric systems // IET Biometrics. 2020. Vol. 9(3). P.91-99. DOI: 10.1049/iet-bmt.2018.5265.

[48] ***Nandakumar K., Chen Y., Dass C., Jain A.K.*** Likelihood ratio based biometric score fusion // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2007. P.1-9.

[49] ***Ross A., Jain A.K.*** Fusion techniques in multibiometric systems // Face Biometrics for Personal Identification. 2007. P.185-212.

[50] ***Coşkun M., Uçar A., Yildirim Ö., Demir Y.*** Face recognition based on convolutional neural network // 2017 International Conference on Modern Electrical and Energy Systems (MEES). 2017. P.376-379.

[51] ***Уздяев М.Ю., Яковлев Р.Н., Дударенко Д.М., Жебрун А.Д.*** Идентификация человека по походке в видеопотоке // *Известия Юго-Западного государственного университета*. 2020. №24(4). С.57-75. DOI: 10.21869/2223-1560-2020-24-4-57-75.

[52] ***Sokolova A., Konushin A.*** Pose-based deep gait recognition // IET Biometrics. 2019. Vol.8. P.134-143. DOI: 10.48550/arXiv.1710.06512.
[53] ***Ivanna T., Iwan S., Andreas F.*** Face recognition between two person using kernel principal component analysis and support vector machines. *International Journal on Electrical Engineering and Informatics*. 2010. Vol.2. P.53-61. DOI:10.15676/ijeei.2010.2.1.5.
[54] ***Maret Y., Oberson D., Gavrilova M.*** Real-time embedded system for gesture recognition // 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC). 2018. P.30-34. DOI: 10.1109/SMC.2018.00014.
[55] ***Chia-Feng, Chung-Wei Liang, Lee Chiung-Ling, Chung I-Fang*** Vision-based human body posture recognition using support vector machines // Proceedings: 4th International Conference on Awareness Science and Technology. 2012. P.150-155. DOI:10.1109/iCAwST.2012.6469605.
[56] ***Мокеев А.В., Мокеев В.В.*** Об эффективности распознавания лиц с помощью линейного дискриминантного анализа и метода главных компонент // *Вестник Южно-Уральского государственного университета. Компьютерные технологии, автоматическое управление, радиоэлектроника*. 2013. Vol.13. No.3. P.61-70.
[57] ***Струкова О.В.***, ***Ширипова Л.В., Мясников Е.В.*** Распознавание личности по походке: опыт использования метода главных компонент и машины опорных векторов // *Информационные технологии и нанотехнологии*: сб. тр. IV междунар. конф. и молодеж. школы (ИТНТ-2018). Самара: Новая техника, 2018. С.822-832.
[58] ***Li C., Diao Y., Ma H., Li Y.*** A Statistical PCA method for face recognition // Intelligent Information Technology Application. 2008. P.376-380.
[59] ***Nefian Ara, Hayes Monson.*** Face detection and recognition using hidden Markov models. 1998. Vol.1. P.141-145.

Сведения об авторе

Колоденкова Анна Евгеньевна, 1982 г. рождения. Окончила Уфимский государственный авиационный технический университет в 2004 г., д.т.н. (2017). Заведующая кафедрой «Информационные технологии» Самарского государственного технического университета. Член Российской ассоциации искусственного интеллекта. В списке научных трудов более 180 работ в области атомной энергетики, программной инженерии, системного анализа, интеллектуальных и биометрических систем, мягких вычислений, экспертной поддержки принятия решений, технической диагностики и мониторинга состояния промышленного оборудования. AuthorID (РИНЦ): 175446; ORCID: 0000-0002-9784-1871; Author ID (Scopus): 57190670136; Researcher ID (WoS): F-1341-2018. *anna82_42@mail.ru.*

Поступила в редакцию 09.01.2023, после рецензирования 05.02.2023. Принята к публикации 16.02.2023.

Scientific article DOI: 10.18287/2223-9537-2023-13-1-55-74

Ontology of human identification by face and body motions in video surveillance systems

© 2023, A.E. Kolodenkova

Samara State Technical University, Samara, Russia

Abstract

At the present stage of advancing information technology, the development of models and recognition methods by body movements and faces in video surveillance systems is a topical problem. This task is essential for security issues, especially at facilities with mass gatherings to counter a terrorism-related crime. The paper presents a classification of the main biometric features and parameters that characterize a potential violator. This classification has been developed for security control systems and access systems of enterprises. A block diagram of merging biometric data and violator recognition by body motions and face which can be used as the basis for the development of security control systems is

proposed. The types of systems and methods of human recognition by body movements and face are considered, their advantages and disadvantages are revealed. It is noted that for accurate violator recognition under a set of biometric features, it is reasonable to use a combination of recognition methods which will allow to make the right decisions regarding the identification of a potential violator. This paper attempts to consider the main aspects related to human recognition by body movements and face in video surveillance in general, in contrast to well-known works devoted to individual biometric features.

Key words: *recognition methods, biometric features, potential violator, security control systems, video surveillance systems, ontology.*

Citation: *Kolodenkova AE.* Ontology of human identification by face and body motions in video surveillance systems [In Russian]. *Ontology of designing*. 2023. 13(1): 55-74. DOI: 10.18287/2223-9537-2023-13-1-55-74.

Conflict of interest: The author declares no conflict of interest.

List of figures and tables

References

[1] Portal of legal statistics of the Prosecutor General's Office of the Russian Federation, 60 p. http://crimestat.ru/analytics.

[2] A typical model of the actions of a violator who commits a terrorist-oriented crime at an educational facility in the forms of an armed attack, placement of an explosive device, hostage-taking [In Russian]. 41 p. https://minobrnauki.gov.ru.

[3] ***Zenov AYu.*** An integrated approach to the detection, classification and recognition of an intruder in a protected area [In Russian]. *News of higher educational institutions. Volga region. Technical sciences*. 2012; 2 (22): 23-32.

[4] ***Smirnov AM.*** On the question of a fundamental theoretical model for studying the personality of a criminal [In Russian]. *Humanities, socio-economic and social sciences* 2020; 1: 1-5. DOI: 10.23672/SAE.2020.1.53256.

[5] ***Kim EV, Ri PG.*** Criminal identity: criminological analysis [In Russian]. *Scientific notes of TOGU*. 2013; 4:402-407.

[6] ***Abeltsev SN.*** On the identity of the criminal and the practical significance of its study [In Russian]. *Bulletin of the Tambov University. Humanities*. 2000; 3 (19): 83-85.

[7] ***Kopylova GK, Prozorov AV.*** Psychology in the activities of internal affairs bodies [In Russian]. Moscow: Central Committee of the Ministry of Internal Affairs of Russia, 2006. 236 p.

[8] ***Gerasimenko VA.*** Fundamentals of information protection in AS [In Russian]. Moscow: Nauka, 2001. 178 p.

[9] ***Olshansky DV.*** Psychology of terrorism [In Russian]. Moscow: Yurayt, 2015. 194 p.

[10] ***Stukolova LS, Zakirova DA.*** Psychology of modern terrorism [In Russian]. *Alley of Science*. 2018; 5: 546-549.

[11] ***Jain AK, Ross A, Prabhakar S.*** An introduction to biometric recognition // *IEEE Trans. Circuits Syst. Video Technol* 2004; 14: 4-20. DOI: 10.1109/TCSVT.2003.818349.

[12] ***Gazizullin AI.*** Criminological characteristics of the personality of a terrorist of our time [In Russian]. NovaInfo.Ru 2018; 1: 161-165. DOI: 10.24411/2312-0444-2021-4-292-297.

[13] ***Arenova LK, Nabieva EA.*** Personality of a person who committed an act of terrorism [In Russian]. *Actual problems of law and the state in the XXI century*. 2018; 10: 38-46.

[14] ***Primakova OG.*** The identity of the criminal terrorist [In Russian] *Victimology*. 2018; 4 (18): 54-58.

[15] ***Tarchokov BA.*** Motivational features of youth involvement in terrorist activities [In Russian]. *Historical and socio-educational though*.t 2015; 6: 211-213 DOI: 10.17748/2075-9908-2015-7-6/1-211-213.
[16] ***Shendra SE, Khanin AA, Voyloshnikov AD.*** Psychological portrait of a terrorist's personality [In Russian]. *Young scientist.* 2022; 13.1 (408.1): 32-33.
[17] ***Maleeva M, Klenikova E, Martynova Ya.*** Psychological portrait of a terrorist [In Russian]. 7 p. https://scienceforum.ru/2017/article/2017038036.
[18] ***Lepeshkin NYa, Vasilin VG, Obirin AI, Talynev VE.*** Psychological foundations of terrorism and anti-terrorist activity in modern conditions [In Russian]. Educational and methodological manual. - Khabarovsk: Khabarovsk Border Institute of the Federal Security Service of the Russian Federation, 2008, 348 p.
[19] ***Bouchrika I, Jain S, Arora S, Singh UP.*** A Survey of using biometrics for smart visual surveillance: gait recognition. *Advanced Sciences and Technologies for Security Applications*. 2018: 3-23. DOI:10.1007/978-3-319-68533-5_1.
[20] ***Singh JP.*** Vision-based gait recognition: a survey. *IEEE Access*. 2018; 6: 70497-70527. DOI: 10.1109/ACCESS.2018.2879896.
[21] ***Priyanka S, Kaur M.*** Classification in pattern recognition: a review. *IJARCSSE All Rights Reserved* 2013; 3: 298-306.
[22] ***Kobets PN.*** On the complex study of the personality of a criminal in domestic criminology [In Russian]. Problems of personality development: mater. international scientific-practical. conf. Prague, 2013: 93-95.
[23] ***Averyanova TV, Belkin RS, Koruhov YG, Rossinskya ER.*** Criminalistics: textbook for universities [In Russian]. - Moscow: NORMA, 2001. 908 p.
[24] ***Ryszard C.*** Multimodal biometrics for person authentication. 2020, 516 p. https://www.researchgate.net/publication/345480873_Multimodal_Biometrics_for_Person_Authentication. DOI: 10.5772/intechopen.85003.
[25] ***Evans N., Marcel S., Ross A., Teoh ABJ*** Biometrics security and privacy protection // IEEE Signal Process Mag. 2015; 32(5): 17-18. DOI: 10.1109/MSP.2015.2443271.
[26] ***Anil K.Jain, Nandakumar Karthik, Ross Arun*** 50 years of biometric research: Accomplishments, challenges, and opportunities // Pattern Recognition Letters 2016; 79: 80-105. DOI:10.1016/j.patrec.2015.12.013.
[27] Forensic examination of external signs of a person (habitoscopy). Physiognomy of a murderer or how to identify a criminal by appearance: a verbal portrait with a full description [In Russian]. 31 p. https://lehre.ru/do/kriminalisticheskoe-issledovanie-vneshnih-priznakov-cheloveka-gabitoskopiya.html.
[28] ***Fedyunina AP.*** Identification of characterological signs and drawing up a psychological portrait of a possible violator and a loyal employee in the field of information security [In Russian]. Bulletin of AGTU 2007; 4: 231-236.
[29] Verbal portrait. Description of a person's appearance by the method of verbal portrait. Verbal description of a person's appearance criminology [In Russian]. https://goaravetisyan.ru/slovesnyi-portret-opisanie-vneshnosti-cheloveka-po-metodu-slovesnogo.
[30] ***Akimov AA, Mustafina SA.*** Review of modern artificial intelligence methods for recognizing deviant behavior of an individual [In Russian]. Bulletin of the Technological University 2020; 8: 69-79.
[31] ***Almas M. N. Siddiqui, Rupali Telgad, Prapti D. Deshmukh*** Multimodal biometric systems: study to improve accuracy and performance // International Journal of Current Engineering and Technology 2014; 4: 165-171.
[32] ***Gad R., Nawal El-Fishawy, Ayman El-Sayed, Zorkany M.*** Multi-biometric systems: a state of the art survey and research directions. *International Journal of Advanced Computer Science and Applications* 2015; 6(6): 128-138. DOI: 10.14569/IJACSA.2015.060618.
[33] ***Ayodele Oloyede, Aderonke Adegbenjo.*** Current practices in information fusion for multimodal biometrics // American Journal of Engineering Research (AJER) 2017; 6: 148-154.
[34] ***Kovalev SM, Kolodenkova AE, Snasel V.*** Intelligent data fusion technologies in the diagnosis of technical objects [In Russian]. Design Ontology 2019; 1(31): 152-168. DOI: 10.18287/2223-9537-2019-9-1-152-168.
[35] ***Dolgiy AI, Kolodenkova AE, Kovalev SM.*** Problems and methods of merging heterogeneous data in hybrid intelligent systems [In Russian]. Hybrid and synergetic intelligent systems 2018: 181-187.
[36] ***Ailon N., Charikar M., Newman A.*** Aggregating inconsistent information: ranking and clustering // In Proceedings of 37th Annual ACM Symposium on Theory of Computing (STOC) 2015: 684-693.
[37] ***AlMahafzah H, AlRwashdeh MZ.*** A Survey of multibiometric systems // International Journal of Computer Applications 2012; 43: 36-43.
[38] ***Mohamed Soltane, Mimen Bakhti.*** Multi-modal biometric authentications: concept issues and applications strategies. *International Journal of Advanced Science and Technology* 2012; 48: 1-38.
[39] ***Sathish G., Saravanan SV, Narmadha S, Maheswari SU.*** Multi-algorithmic iris recognition. *International Journal of Computer Applications* 2012; 38: 13-21.
[40] ***Mwaura GW, Mwangi W, Otieno C.*** Multimodal biometric system: fusion of face and fingerprint biometrics at match score fusion level // International Journal of Scientific & Technology Research 2017; 6: 41-49.

[41] ***Arun Ross, Anil Jain*** Information fusion in biometrics // Pattern Recognition Letters 2003: 2115-2125.
[42] ***Delac K, Grgic M.*** A Survey of biometric recognition methods // 46th International Symposium, ELMAR-2004, 2004: 184-193.
[43] ***Aly OM, Salama GI, Mahmoud TA, Onsi HM.*** A multimodal biometric recognition system using feature fusion based on PSO // International Journal of Advanced Research in Computer and Communication Engineering 2013;. 2: 4336-4343. DOI:10.1007/s10916-019-1391-5.
[44] ***Ghayoumi M.*** A review of multimodal biometric systems: fusion methods and their applications // IEEE/ACIS 14th International Conference Computer and Information Science (ICIS) 2015: 131-136. DOI: 10.1109/ICIS.2015.7166582.
[45] ***Radha N***, ***Kavitha A.*** Rank level fusion using fingerprint and iris biometrics // Indian Journal of Computer Science and Engineering (IJCSE) 2011; 2; 917-923.
[46] ***Haryati Jaafar, Dzati Athiar Ramli*** A review of multibiometric system with fusion strategies and weighting factor // International Journal of Computer Science Engineering (IJCSE) 2013; 2: 158-165.
[47] ***Abderrahmane H, Noubeil G, Ziet L, Zahid A, Dipankar D.*** Weighted quasi-arithmetic mean based score level fusion for multi-biometric systems. *IET Biometrics* 2020; 9(3): 91-99. DOI: 10.1049/iet-bmt.2018.5265.
[48] ***Nandakumar K., Chen Y., Dass C., Jain A.K.*** Likelihood ratio based biometric score fusion // IEEE Transactions on Pattern Analysis and Machine Intelligence 2007: 1-9.
[49] ***Ross A., Jain A.K.*** Fusion techniques in multibiometric systems // Face Biometrics for Personal Identification 2007; 185-212.
[50] ***Coşkun M, Uçar A, Yildirim Ö, Demir Y.*** Face recognition based on convolutional neural network // 2017 International Conference on Modern Electrical and Energy Systems (MEES) 2017: 376-379.
[51] ***Uzdyaev MYu, Yakovlev RN, Dudarenko DM, Zhebrun AD.*** Identification of a person by gait in a video stream [In Russian]. Proceedings of the Southwestern State University 2020; 24(4): 57-75. DOI: 10.21869/2223-1560-2020-24-4-57-75.
[52] ***Sokolova A, Konushin A.*** Pose-based deep gait recognition // IET Biometrics 2019; 8: 134-143. DOI: 10.48550/arXiv.1710.06512.
[53] ***Timotius Ivanna, Setyawan Iwan, Febrianto Andreas*** Face recognition between two person using kernel principal component analysis and support vector machines // International Journal on Electrical Engineering and Informatics 2010; 2: 53-61. DOI:10.15676/ijeei.2010.2.1.5.
[54] ***Maret Y., Oberson D., Gavrilova M.*** Real-time embedded system for gesture recognition // 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC) 2018: 30-34. DOI: 10.1109/SMC.2018.00014.
[55] ***Chia-Feng, Chung-Wei Liang, Lee Chiung-Ling, Chung I-Fang*** Vision-based human body posture recognition using support vector machines // Proceedings: 4th International Conference on Awareness Science and Technology 2012: 150-155. DOI: 10.1109/iCAwST.2012.6469605.
[56] ***Mokeev AV, Mokeev VV.*** On the effectiveness of facial recognition using linear discriminant analysis and the method of principal components [In Russian]. *Bulletin of the South Ural State University. Computer technology*, automatic control, radio electronics 2013; 13: 61-70.
[57] ***Strukova OV, Shiripova LV, Myasnikov EV.*** Personality recognition by gait: the experience of using the principal component method and the support vector machine [In Russian]. *Information technologies and nanotechnologies* 2018: 822-832.
[58] ***Li C, Diao Y, Ma H, Li Y.*** A Statistical PCA Method for Face Recognition. Intelligent Information Technology Application 2008: 376-380.
[59] ***Nefian Ara, Hayes Monson*** Face detection and recognition using hidden Markov models 1998; 1: 141-145.

About the author

Anna Evgenievna Kolodenkova (b. 1982) graduated from the Ufa State Aviation Technical University (Ufa-city) in 2004, D. Sc. Eng. (2017). She is an Associate Professor and the Head of «Information technologies» Department at Samara State Technical University. She is a member of Russian Association of Artificial Intelligence. She is a co-author of about 180 scientific articles and abstracts in the field of nuclear energy, software engineering, system analysis, intelligent and biometric systems, soft computing, expert decision support and technical diagnostics and monitoring of industrial equipment condition. AuthorID (RCI): 175446. ORCID: 0000-0002-9784-1871. Author ID (Scopus): 57190670136; Researcher ID (WoS): F-1341-2018. *anna82_42@mail.ru.*

Received January 9, 2023. Revised February 05, 2023. Accepted February 16, 2023.