Дата поступления рукописи в редакцию: 25.08.2026 г.
Дата принятия рукописи в печать: 01.10.2026 г.
DOI: 10.24412/2224-9133-2026-9-220-224

ЦАРЬКОВА Евгения Геннадьевна,
кандидат физико-математических наук,
доцент, ведущий научный сотрудник
ФКУ НИИ ФСИН России,
e-mail: university69@mail.ru

ИДЕНТИФИКАЦИЯ ОСУЖДЕННЫХ ПО ЧАСТОТЕ ШАГА В СИСТЕМАХ ОХРАНЫ УЧРЕЖДЕНИЙ УИС: ТЕХНОЛОГИЧЕСКИЕ ВОЗМОЖНОСТИ И ПРАВОВЫЕ ОГРАНИЧЕНИЯ

Аннотация. *В статье рассматриваются возможности применения технологий идентификации осужденных по характеристикам походки в целях снижения прогнозируемых рисков нарушения установленного порядка отбывания наказания и обеспечения безопасности в учреждениях уголовно-исполнительной системы Российской Федерации (УИС). Обосновывается, что анализ частоты и ритма шага, продолжительности шагового цикла, скорости передвижения, траектории движения, силуэта и иных динамических параметров ходьбы позволяет бесконтактно сопоставлять наблюдаемого человека с ранее сформированным биометрическим профилем. Технология может использоваться для своевременного выявления несоответствия между личностью лица, фактически находящегося в контролируемой зоне, и сведениями системы учета либо контроля доступа, а также для повышения достоверности данных о перемещениях осужденных в зонах, связанных с повышенным риском побега, несанкционированного доступа, конфликтного взаимодействия или нарушения режима. Показано, что частота шага не обладает достаточной индивидуализирующей способностью при изолированном использовании и должна рассматриваться только как один из компонентов многомодальной идентификационной системы, объединяющей видеоаналитику, параметры походки, контуры тела, сведения о маршрутах и данные системы контроля доступа. Особое внимание уделяется правовым ограничениям обработки динамических биометрических данных: необходимости определения цели и пределов их использования, валидации алгоритмов на профильной выборке, защиты информации, сохранения контроля со стороны должностного лица и недопустимости принятия юридически значимых решений исключительно на основании автоматизированного сопоставления биометрических признаков.*

Ключевые слова: *искусственный интеллект, компьютерное зрение, идентификация по походке, частота шага, биометрические персональные данные, уголовно-исполнительная система Российской Федерации, система охраны, видеоаналитика, машинное обучение, контроль доступа, алгоритмическая валидация, права осужденных.*

TSARKOVA Evgeniya Gennadievna,
candidate of Physical and Mathematical Sciences,
associate professor, Leading Researcher of the
Federal Research Institute of the Federal Penitentiary
Service of Russia

IDENTIFICATION OF CONVICTS BASED ON STEP FREQUENCY IN SECURITY SYSTEMS OF PENITENTIARY INSTITUTIONS: TECHNOLOGICAL CAPABILITIES AND LEGAL RESTRICTIONS

Annotation. *The article examines the possibilities of using gait-based identification technologies for convicts in order to reduce the projected risks of violating the established order of serving their sentence and to ensure safety in institutions of the Penal System of the Russian Federation (PS). It is substantiated that the analysis of the frequency and rhythm of steps, the duration of the step cycle, the speed of movement, the trajectory of movement, the silhouette, and other dynamic parameters of walking makes it possible to*

non-contactingly compare the observed person with a previously created biometric profile. The technology can be used to promptly identify discrepancies between the identity of a person actually present in a controlled area and the data in the accounting or access control system, as well as to improve the reliability of data on the movements of convicts in areas associated with an increased risk of escape, unauthorized access, conflict interaction, or violation of the regime. It has been shown that stride frequency does not have sufficient individualizing capacity when used in isolation and should be considered only as one component of a multimodal identification system that combines video analytics, gait parameters, body contours, route information, and data from the access control system. Special attention is paid to the legal restrictions on the processing of dynamic biometric data: the need to define the purpose and limits of its use, the validation of algorithms on a specialized sample, the protection of information, the maintenance of control by an official, and the inadmissibility of making legally significant decisions solely based on automated comparison of biometric features.

Key words: *artificial intelligence, computer vision, gait identification, stride frequency, biometric personal data, the Penal System of the Russian Federation, security system, video analytics, machine learning, access control, algorithmic validation, the rights of convicts.*

Охрана и надзор в учреждениях уголовно-исполнительной системы Российской Федерации (УИС) традиционно опираются на физические посты, инженерно-технические средства, видеонаблюдение, пропускной режим и учет перемещений [1, С.114; 2, С.54]. Эти механизмы позволяют фиксировать уже произошедшее событие или устанавливать личность при непосредственном визуальном наблюдении. Однако в протяженных коридорах, производственных помещениях, прогулочных дворах, переходах и иных зонах учреждения сотрудник не всегда способен оперативно сопоставить наблюдаемого человека с конкретным осужденным. В этих условиях возрастает значение бесконтактных способов установления личности [3, С.64]. К ним относится распознавание по походке – направлению биометрической идентификации, использующему устойчивые особенности движения человека. В отличие от отпечатка пальца, радужной оболочки или изображения лица, походка может анализироваться на расстоянии и без обязательного взаимодействия лица с устройством [4, С.329]. Технология потенциально применима в ситуациях, когда лицо частично закрыто, находится на удалении от камеры либо движется в зоне, где использование традиционной процедуры идентификации затруднено.

Частота шага представляет собой число шагов, совершаемых человеком за единицу времени, либо характеристику периодичности шагового цикла. Она связана с индивидуальной манерой передвижения, длиной шага, скоростью, координацией движений и физиологическими параметрами. Вместе с тем частота шага является лишь одним из компонентов походки. В научных обзорах распознавание по походке обычно рассматривается как использование совокупности пространственных, временных, кинематических, инерциальных и частотных признаков, а не как идентификация по одному числовому параметру.

Для использования частоты шага в системе охраны требуется последовательная обработка видеосигнала или данных других сенсоров. На первом этапе камера либо иной датчик фиксирует перемещение человека. Затем алгоритм выделяет фигуру из фона, отслеживает ее по кадрам, оценивает траекторию движения и определяет моменты постановки ног или повторяющиеся фазы шагового цикла. На основании этих данных рассчитываются частота шага, продолжительность цикла, вариативность ритма, скорость движения и иные параметры. Видеосистема может работать в двух основных режимах: в режиме верификации (когда система сопоставляет походку лица с заранее выбранным профилем и отвечает на вопрос, соответствует ли наблюдаемый человек заявленной личности) и в режиме идентификации (когда признаки походки сравниваются с базой профилей для поиска наиболее вероятного соответствия).

В условиях деятельности учреждений УИС наиболее реалистичным является не автономный поиск личности по одной частоте шага, а сценарий риск-ориентированного сопоставления. Например, система может обнаружить, что в служебной зоне перемещается человек, чьи ростовые, силуэтные и динамические признаки не соответствуют разрешенному для этой зоны лицу. В таком случае алгоритм формирует сигнал оператору, а сотрудник проводит дополнительную проверку с использованием визуального контроля, данных пропускной системы либо иных предусмотренных процедур.

Практическая ценность частоты шага состоит в возможности фильтрации и приоритезации видеопотока. В учреждении, где камеры формируют значительный объем данных, система способна выделять нестандартные паттерны движения: ускоренное перемещение, резкое изменение ритма, длительное нахождение в запрещенной

зоне, попытку следовать за другим лицом через контролируемый проход или несоответствие динамического профиля данным учетной записи. Такое использование не означает, что частота шага сама по себе подтверждает личность; она лишь участвует в формировании сигнала о необходимости проверки.

Перспективным является объединение частоты шага с другими признаками. В качестве элементов комбинированной модели могут использоваться геометрия и силуэт тела, извлекаемые из видеопоследовательности; длина шага, ширина постановки ног, симметрия движений и фазовая структура ходьбы; скорость и траектория перемещения в контролируемой зоне; данные электронного пропуска, времени прохода и разрешенного маршрута; результаты визуальной идентификации сотрудником; при наличии законного основания – иные биометрические признаки, используемые в пределах установленной цели обработки [4, С.329; 5, С.120]. Такой подход позволяет снизить зависимость результата от одного нестабильного параметра. Частота шага может дополнить оценку, но не должна подменять собой полноценную биометрическую идентификацию.

Основной технологический риск применения рассматриваемой технологии заключается в вариативности походки. Частота шага зависит не только от относительно устойчивых физиологических характеристик человека, но и от множества внешних и ситуативных факторов. На нее влияют покрытие пола, уклон, освещенность зоны, обувь, одежда, переносимые предметы, физическая усталость, травма, заболевание, возрастные изменения, эмоциональное состояние, скорость передвижения и наличие препятствий. Исследования распознавания походки указывают на чувствительность систем к изменениям условий движения, одежды, ракурса камеры и других ковариат [6, С.3;

7, С.10]. Поэтому совпадение частоты шага с параметрами профиля не подтверждает личность с требуемой степенью достоверности. Равным образом отклонение от ранее зафиксированного ритма ходьбы не свидетельствует о подмене лица или попытке нарушения режима. Осужденный может изменить манеру передвижения по медицинским, бытовым или психологическим причинам. Лицо, намеренно имитирующее походку другого человека, также способно приблизиться к отдельным параметрам, особенно если система использует ограниченный набор признаков.

Дополнительные сложности возникают при видеонаблюдении в реальной обстановке. Камера может фиксировать человека под неудобным углом, при перекрытии фигуры другими лицами, в условиях плохого освещения либо при кратковременном фрагменте движения. Для надежного выделения циклических характеристик необходима достаточно продолжительная и качественная последовательность шагов. Обзор методов на основе инерциальных датчиков отмечает, что для практического распознавания требуется наблюдение нескольких шагов, а качество заметно зависит от стабильности условий регистрации. Поэтому использование частоты шага в УИС должно основываться на презумпции ограниченной достоверности. Алгоритм может выявить аномалию или предложить вероятностное совпадение, однако окончательный вывод о личности человека, наличии нарушения либо необходимости применения меры реагирования должен приниматься сотрудником после проверки совокупности обстоятельств.

При этом использование частоты шага для установления личности осужденного имеет особый правовой режим. Сведения о движении человека становятся биометрическими персональными данными, когда оператор обрабатывает их с целью идентификации конкретного лица с применением специальных технических средств [8, С.12; 9, С.495]. Именно целевое использование походки для установления личности определяет необходимость применения повышенных гарантий защиты. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» относит к биометрическим персональным данным сведения, характеризующие физиологические и биологические особенности человека, на основе которых может быть установлена его личность, если оператор использует их для идентификации. Закон предусматривает общее правило письменного согласия на обработку биометрических данных, но также устанавливает исключения [10, С.314]. Наличие такого исключения не отменяет обязанности определить конкретную цель, правовое основание, объем обработки и меры защиты данных.

Для УИС это означает, что применение технологии не может быть обосновано лишь общей ссылкой на задачу обеспечения безопасности. Требуется нормативно определить как минимум, какие именно параметры походки собираются и каким образом они преобразуются в биометрический шаблон; в каких зонах учреждения и для каких задач допускается видеосбор и алгоритмический анализ; какие должностные лица имеют доступ к исходной видеозаписи, шаблону походки и результатам сопоставления; каковы сроки хранения, основания удаления и порядок актуализации биометрического профиля; как обеспечиваются журналирование доступа, защита от несанкционированного копирования и передача данных; в каких случаях алгоритмический сигнал требует обязательной проверки человеком; как лицо может получить сведения о неблагоприятном выво-

де и обжаловать последствия его использования.

Особое ограничение связано с автоматизированным принятием юридически значимых решений. Если результат сопоставления по походке непосредственно приводит к постановке на профилактический учет, применению дисциплинарного взыскания, ограничению перемещений, отказу в доступе к разрешенной зоне либо иной неблагоприятной мере, то система фактически влияет на правовой статус осужденного. В такой ситуации недопустимо превращать вероятностный вывод алгоритма в единственное и достаточное доказательство.

Надлежащая модель предполагает разделение автоматизированного анализа и управленческого решения. Система вправе сформировать технический сигнал (например, о несоответствии наблюдаемого динамического профиля профилю лица, прошедшего через контрольную точку). Но этот сигнал должен иметь ориентирующий статус. Он требует проверки оператором, сопоставления с видеозаписью, данными пропускного режима, сведениями о состоянии здоровья, объяснениями лица и иными фактическими обстоятельствами. Только после такой проверки уполномоченное должностное лицо может принять решение, предусмотренное законом. Дополнительно необходима оценка пропорциональности обработки. Непрерывное создание индивидуальных профилей походки всех осужденных во всех пространствах учреждения может оказаться избыточным по отношению к цели охраны. Более обоснованным является применение технологии в зонах повышенного режима: на контрольно-пропускных пунктах, в коридорах служебного доступа, у периметра, в местах пересечения маршрутов, в технических помещениях и иных участках, где требуется подтвердить соответствие лица разрешенному маршруту. При этом следует минимизировать сбор данных, не связанных с задачей идентификации и предотвращения конкретных угроз.

Внедрение идентификации по частоте шага в системе охраны УИС целесообразно осуществлять поэтапно. На первом, исследовательском, этапе следует использовать обезличенные или надлежащим образом защищенные архивные записи для проверки возможности выделения параметров ходьбы в конкретной инфраструктуре учреждения. Целью здесь является не принятие решений в отношении лиц, а оценка качества алгоритма в реальных условиях: при разной освещенности, одежде, скорости движения и ракурсах камер.

На этапе пилотного внедрения допустимо применять систему как инструмент технического оповещения оператора. Алгоритм может фиксировать несоответствие динамических признаков профилю, обнаруживать нестандартный маршрут или отмечать аномальную активность в контролируемой зоне. Результат не должен автоматически ограничивать права лица.

На эксплуатационном этапе технология может использоваться только как составная часть многомодальной системы охраны. Частота шага должна объединяться с данными видеонаблюдения, контроля доступа и профессиональной оценкой сотрудника. Для каждой модели необходимы регулярная валидация, документирование ошибок, контроль ложноположительных и ложноотрицательных результатов, а также независимый аудит условий эксплуатации.

Нормативная регламентация должна закрепить запрет на применение частоты шага как единственного идентификатора или самостоятельного основания для дисциплинарной, профилактической либо иной ограничительной меры. Также необходимо установить порядок информирования о применяемой технологии в пределах, совместимых с требованиями безопасности, процедуры внутреннего контроля, правила рассмотрения жалоб и ответственность за неправомерную обработку биометрических данных.

Частота шага может быть полезным динамическим параметром для повышения эффективности охраны учреждений УИС, прежде всего при автоматизированном анализе видеопотока и выявлении ситуаций, требующих внимания оператора. Однако эта характеристика не обладает достаточной устойчивостью и индивидуализирующей силой, чтобы выступать самостоятельным средством достоверной идентификации осужденного. Ее применение допустимо лишь в составе комплексной системы, сочетающей несколько источников информации и сохраняющей решающую роль человека. Правовая допустимость технологии зависит от четко определенной цели обработки, соблюдения режима биометрических персональных данных, минимизации объема наблюдения, надежной защиты информации, предварительной валидации алгоритмов и недопущения автоматического принятия решений, ухудшающих правовое положение осужденного. Такой подход позволяет совместить интересы безопасности учреждения с требованиями законности, соразмерности и защиты прав человека.

Список литературы:

[1] Денисенко О. И., Жаров И. С., Кадралеева Ж. А. Использование систем идентификации личности для обеспечения безопасности на режимных объектах уголовно-исполнительной системы // Вестник Самарского юридического института ФСИН России. 2024, № 4. С. 113-119.

[2] Царькова Е.Г. Учебная аналитика в дистанционном обучении: особенности применения и перспективы развития // Прикладная психоло-

гия и педагогика. 2022, Т. 7, № 3. С. 54-66.

[3] Шиняев К.А., Морозов А.С. Современные цифровые технологии в системе надзора следственных изоляторов уголовно-исполнительной системы Российской Федерации // Вестник Самарского юридического института. 2025, № 4 (65). С. 62-66.

[4] Пекарева В.В., Фроловская Ю.И. Искусственный интеллект в уголовно-исполнительной системе // Право и государство: теория и практика. 2024, № 10. С. 329-331.

[5] Курдюкова Е.А., Романченко М.Д. Искусственный интеллект в деятельности уголовно-исполнительной системы // Современное право. 2023. № 10. С. 119–121.

[6] Андреева Е.А., Беляев А.К., Еремин Ю.М., Царькова Е.Г. Методы биометрической идентификации на основе применения нейросетевых технологий // Информационные технологии в УИС. 2019. № 3. С. 2-10.

[7] Чураков Д.Ю., Царькова Е.Г., Беляев А.К. Точный расчет: возможности автоматизации при проведении оценки эффективности системы безопасности охраняемых объектов УИС // Информационные технологии в УИС. 2020. № 2. С. 10-21.

[8] Талапина Э.В. Прозрачность алгоритмов искусственного интеллекта // Право. Журнал Высшей школы экономики. 2025. Т. 18. № 3. С. 4–27.

[9] Зорина Н.С., Царькова Е.Г. Особенности психологической коррекции личности несовершеннолетних осужденных // Евразийский юридический журнал. 2024. № 11(198). С. 494-495.

[10] Зорина Н.С., Царькова Е.Г. Правонарушения в сети Интернет: классификация, возникающие риски и меры предотвращения // Евразийский юридический журнал. 2024. № 6(193). С. 313-314.

References:

[1] Denisenko O. I., Zharov I. S., Kadraleeva Zh. A. Use of personal identification systems to ensure security at secure facilities of the penitentiary system // Bulletin of the Samara Law Institute of the Federal Penitentiary Service of Russia. 2024, № 4. S. 113-119.

[2] Tsarkova E.G. Educational analytics in distance learning: features of application and development prospects // Applied psychology and pedagogy. 2022, VOL. 7, NO. 3. S. 54-66.

[3] Shinyaev K.A., Morozov A.S. Modern digital technologies in the system of supervision of pre-trial detention centers of the penitentiary system of the Russian Federation // Bulletin of the Samara Law Institute. 2025, № 4 (65). S. 62-66.

[4] Pekareva V.V., Frolovskaya Yu.I. Artificial intelligence in the penal system // Law and the state: theory and practice. 2024, № 10. S. 329-331.

[5] Kurdyukova E.A., Romanchenko M.D. Artificial intelligence in the activities of the penitentiary system // Modern law. 2023. № 10. S. 119-121.

[6] Andreeva E.A., Belyaev A.K., Eremin Yu.M., Tsarkova E.G. Methods of biometric identification based on the use of neural network technologies // Information technologies in UIS. 2019. № 3. S. 2-10.

[7] Churakov D.Yu., Tsarkova E.G., Belyaev A.K. Accurate calculation: possibilities of automation when assessing the effectiveness of the security system of protected objects of the penal system // Information technologies in the penal system. 2020. № 2. S. 10-21.

[8] Talapina E.V. Transparency of artificial intelligence algorithms // Law. Journal of the Higher School of Economics. 2025. T. 18. № 3. S. 4-27.

[9] Zorina N.S., Tsarkova E.G. Features of psychological correction of the personality of juvenile convicts // Eurasian Law Journal. 2024. № 11(198). S. 494-495.

[10] Zorina N.S., Tsarkova E.G. Offenses on the Internet: classification, emerging risks and preventive measures // Eurasian Legal Journal. 2024. № 6(193). S. 313-314.