

УДК 004.056.5

DOI: [10.26102/2310-6018/2025.49.2.040](https://doi.org/10.26102/2310-6018/2025.49.2.040)

Аутентификация пользователей на основе анализа длины и временных параметров рукописной подписи

Р.Н. Дзямко-Гамулец✉, О.П. Иевлев

*Московский технический университет связи и информатики, Москва,
Российская Федерация*

Резюме. В работе представлены методы для аутентификации пользователя на основе признаков рукописной подписи, характеризующих ее длину как скалярную величину, так и функцию зависимости длины кривой части подписи от времени. Основной акцент делается на методах выделения статических и динамических признаков из рукописной подписи, данные признаки являются уникальными для каждого человека и могут быть использованы для принятия истинности или ложности конкретного пользователя. В процессе анализа собираются данные о временных характеристиках, включая время, затраченное на написание каждого символа, и паузы между отдельными элементами подписи. Актуальность данного исследования обусловлена необходимостью повышения уровня безопасности аутентификации пользователей в различных системах, где рукописная подпись служит важным элементом аутентификации. Результаты исследования могут быть полезны для создания более надежных систем аутентификации в таких сферах, как банковское дело, правовые процедуры, а также в других областях, где требуется высокая степень уверенности в подлинности документов. Представленные подходы не только способствуют повышению уровня безопасности авторизации, но также расширяют горизонты для дальнейших исследований в сфере биометрической аутентификации. Это, в свою очередь, может привести к более широкому внедрению данных технологий в практическое применение как в онлайн, так и офлайн системах.

Ключевые слова: математическое ожидание, дисперсия, функция, рукописная подпись, аутентификация, мера, метрика, производная, машинное обучение.

Для цитирования: Дзямко-Гамулец Р.Н., Иевлев О.П. Аутентификация пользователей на основе анализа длины и временных параметров рукописной подписи. *Моделирование, оптимизация и информационные технологии.* 2025;13(2). URL: <https://moitvvt.ru/ru/journal/pdf?id=1929>
DOI: 10.26102/2310-6018/2025.49.2.040

User authentication based on analysis of the length and timing parameters of handwritten signature

R.N. Dzyamko-Gamulets✉, O.P. Ievlev

*Moscow Technical University of Communications and Informatics, Moscow,
the Russian Federation*

Abstract. This article presents methods for user authentication based on handwritten signature features characterizing its length as a scalar value and as a function of the dependence of the signature part curve length on time. The main emphasis is on methods for extracting static and dynamic features from a handwritten signature, these features are unique to each person and can be used to accept the truth or falsity of a particular user. During the analysis, data on time characteristics are collected, including the time spent writing each symbol and pauses between individual signature elements. The relevance of this study is due to the need to improve the security of user authentication in various systems where a handwritten signature serves as an important authentication element. The results of the study can be useful for creating more reliable authentication systems in such areas as banking, legal procedures, and other areas where a high degree of confidence in the authenticity of documents is required. The presented

approaches not only contribute to increasing the level of authorization security, but also expand the horizons for further research in the field of biometric authentication. This, in turn, may lead to wider implementation of these technologies in practical applications in both online and offline systems.

Keywords: mathematical expectation, variance, function, handwritten signature, authentication, measure, metric, derivative, machine learning.

For citation: Dzyamko-Gamulets R.N., Ievlev O.P. User authentication based on analysis of the length and timing parameters of handwritten signature. *Modeling, Optimization and Information Technology*. 2025;13(2). (In Russ.). URL: <https://moitvvt.ru/ru/journal/pdf?id=1929> DOI: 10.26102/2310-6018/2025.49.2.040

Введение

Аутентификация на основе рукописной подписи представляет собой процесс проверки подлинности личности человека с использованием его уникального почерка. Рукописная подпись является одним из самых распространенных методов идентификации и аутентификации, поскольку она сочетает в себе как физические, так и поведенческие характеристики. Каждый человек имеет свой индивидуальный стиль написания, который формируется под воздействием множества факторов, таких как культура, образование и личные привычки. В отличие от традиционных методов аутентификации, таких как пароли или PIN-коды, рукописная подпись предоставляет альтернативный способ проверки личности, поскольку, обладая изображением чужой подписи не всегда удастся ее воспроизвести другим лицом. Но это также накладывает дополнительные сложности, обусловленные тем, что рукописная подпись человека не всегда постоянна, а зависит от множества факторов и подвержена изменению со временем в тех или иных пределах [1].

Современные технологии позволяют использовать алгоритмы машинного обучения для анализа и обработки рукописных подписей, что значительно повышает эффективность аутентификации. В частности, исследование признаков, таких как длина подписи и ее временные параметры, открывают новые горизонты в области биометрической аутентификации. Данные методы не только способствуют повышению уровня безопасности, но и позволяют учитывать индивидуальные особенности подписей, что делает процесс аутентификации более надежным и точным. Но важно отметить, что данный подход использует лишь часть информации, поэтому в реальных условиях целесообразно применять его только вместе с другими методами выделения признаков, которые учитывают геометрическую форму подписи, а не только ее одномерное представление в виде функции длины.

Первый этап, который необходим, это сбор подписей в виде множества точек, каждая из которых характеризуется координатами x и y , а также временной меткой написания каждой точки. Здесь можно собирать данные собственными средствами, например, создав приложение, в котором пользователи будут вводить образцы своих подписей и проверять алгоритмы распознавания, или же воспользоваться сторонними открытыми датасетами. Поскольку собранные данные в своем необработанном виде обычно малоприспособлены для анализа и обработки, то сначала необходимо привести эти данные к некоторому более формальному виду [2]. Например, здесь может идти речь о написании подписей на устройствах с различными диагоналями экранов, что влияет на размер подписи. Для корректности сравнения стоит привести все подписи к единому размеру. Также устройства могут быть повернуты под разными углами, что тоже необходимо учитывать.

Процесс предобработки подписи включает создание равномерной сетки временных точек, полученных в результате линейной интерполяции соседних значений,

а также масштабирование и поворот рукописной подписи на заранее определяемый угол. Данные этапы позволяют выделить ключевые признаки, которые в дальнейшем используются для сравнения и оценки близости подписи.

Ранее проведенные эксперименты продемонстрировали, что общее время, затраченное на написание подписи, может служить индикатором для выявления поддельных экземпляров. Очевидно, что значительное отклонение времени написания от ранее обработанных образцов должно вызывать подозрения о ложности тестируемого пользователя. В таких случаях целесообразно запрашивать повторный ввод подписи, что может существенно повысить надежность системы аутентификации [3].

Помимо общего времени написания, важно исследовать подпись как функцию длины от времени. Данная идея основывается на предположении, что при написании одной и той же подписи пользователь будет демонстрировать схожие паттерны изменения скорости написания. В разные моменты времени, автор подписи может замедляться или ускоряться, что создает уникальный ритм и стиль написания, присущий только ему.

Таким образом, скорость изменения длины подписи в зависимости от времени становится своеобразным «отпечатком» руки, который может быть использован для аутентификации пользователя. Это подчеркивает важность анализа не только конечного результата – длины подписи, но и динамики процесса ее написания. Исследование данных характеристик может привести к созданию более совершенных алгоритмов, способных выявлять аномалии и отличать оригинальные подписи от подделок [4].

Материалы и методы

Пусть подпись задана в виде функций координат от времени:

$$\begin{cases} x = x(t) \\ y = y(t) \end{cases} \quad (1)$$

Длина подписи в момент времени t , при условии, что подпись начинается в момент времени t_0 , будет выражаться формулой:

$$\int_{t_0}^t \sqrt{\dot{x}(\tau)^2 + \dot{y}(\tau)^2} d\tau, \quad (2)$$

где $\dot{x}(\tau)$, $\dot{y}(\tau)$ – производные функций координат подписи.

Для вычислений подпись представляется в виде последовательности точек, где каждая точка несет информацию о временной метке написания текущей координате, а также сами значения координат по осям Ox и Oy . В дальнейшем количество точек будет обозначаться как N .

Причем после предобработки предполагается, что данная последовательность точек образует одинаковые интервалы, то есть:

$$x_{i+1} - x_i = x_i - x_{i-1}, \quad (3)$$

для $\forall i \in N \cup \{0\} \cap [0, N - 1]$, где $N \cup \{0\}$ – множество натуральных чисел, включая ноль. Предполагается, что нумерация точек начинается с 0.

Поскольку подпись после предобработки представляется в виде массива точек численность N , то формулы длины выглядят следующим образом:

Левосторонняя численная производная в точке с индексом i :

$$\dot{x}_i = \frac{x_i - x_{i-1}}{t_i - t_{i-1}}, \quad \dot{y}_i = \frac{y_i - y_{i-1}}{t_i - t_{i-1}}. \quad (4)$$

Правосторонняя численная производная:

$$\dot{x}_i = \frac{x_{i+1}-x_i}{t_{i+1}-t_i}, \frac{y_{i+1}-y_i}{t_{i+1}-t_i}. \quad (5)$$

Центральная численная производная:

$$\dot{x}_i = \frac{x_{i+1}-x_{i-1}}{t_{i+1}-t_{i-1}}, \frac{y_{i+1}-y_{i-1}}{t_{i+1}-t_{i-1}}. \quad (6)$$

Что касается численной длины, пусть временное расстояние между точками одинаково и равно $\Delta\tau$, тогда длина кривой в точке с индексом k будет выражаться формулой:

$$l_k = \sum_{i=0}^k \sqrt{\frac{(x_{i+1}-x_i)^2}{(\tau_{i+1}-\tau_i)^2} + \frac{(y_{i+1}-y_i)^2}{(\tau_{i+1}-\tau_i)^2}} \cdot (\tau_{i+1} - \tau_i). \quad (7)$$

Поскольку $\tau_{i+1} - \tau_i = \Delta\tau$ и не зависит от индекса i (так как все интервалы одинаковы), то можно преобразовать в данный вид:

$$l_k = \sum_{i=0}^k \sqrt{\frac{(x_{i+1}-x_i)^2}{\Delta\tau^2} + \frac{(y_{i+1}-y_i)^2}{\Delta\tau^2}} \cdot \Delta\tau. \quad (8)$$

Внесем $\Delta\tau$ под корень и сократим со знаменателями, получим:

$$l_k = \sum_{i=0}^k \sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}. \quad (9)$$

Данная формула может быть интерпретирована как сумма длин хорд ломанной, которая аппроксимирует кривую.

Численная производная функции длины подписи в точке с индексом i будет считаться следующим образом:

$$\dot{l}_i = \frac{l_{i+1}-l_{i-1}}{t_{i+1}-t_{i-1}}. \quad (10)$$

Пусть даны две подписи и $\{x_i^{(1)}\}, \{y_i^{(1)}\}, i=\overline{0..N-1}$ – координаты точек после предобработки первой подписи, а $\{x_i^{(2)}\}, \{y_i^{(2)}\}, i=\overline{0..N-1}$ – второй.

Тогда в качестве меры различия этих двух подписей будет выступать следующая величина:

$$diff = \frac{1}{N} \sum_{i=0}^{N-1} (x_i^{(1)} - x_i^{(2)})^2 + (y_i^{(1)} - y_i^{(2)})^2. \quad (11)$$

Возникает вопрос, как сравнивать две подписи, когда в качестве сравниваемого параметра выступает функция длины от времени каждой из подписей [5]. Нужно сравнить две функции длины на одинаковой нормированной временной шкале, предполагая, что время, затраченное на написание каждой подписи, равно 1.

Пусть имеются функции длин для двух подписей – $l_1(t)$ и $l_2(t)$.

Тогда в качестве меры их различия на интервале $[t_1; t_2]$ можно выбрать следующий функционал:

$$diff = \frac{1}{|t_2-t_1|} \int_{t_1}^{t_2} |l_1(\tau) - l_2(\tau)| d\tau. \quad (12)$$

Для вычисления необходимо представить все имеющиеся данные в виде конечных множеств. Для функций длин подписей в зависимости от времени будем иметь две конечные последовательности из N точек каждая – $\{l_i^{(1)}\}, \{l_i^{(2)}\}, i = \overline{0..N-1}$ мера различия преобразуется в следующий функционал:

$$diff = \frac{1}{N} \sum_{i=0}^{N-1} |l_i^{(1)} - l_i^{(2)}|. \quad (13)$$

Пусть имеются K подписей, для каждой из которых вычислена функция длины от времени – $\{l^{(j)}\}_{j=0}^K$.

Тогда можно ввести понятие усредненной функции длины для этих K подписей, которая выражается следующей формулой:

$$\bar{l}(t) = \frac{1}{K} \sum_{j=0}^{K-1} l^{(j)}(t). \quad (14)$$

Для дискретного случая, когда функции заданы следующими величинами – $\{l_i^{(j)}\}_{j=0}^K$.

Усредненная подпись будет представляться следующим образом:

$$\bar{l}_i = \frac{1}{K} \sum_{j=0}^{K-1} l_i^{(j)}. \quad (15)$$

Для определения меры разброса функций длин подписей, используется функция дисперсии, которая для дискретного случая имеет следующий вид:

$$D_i = \frac{1}{K} \sum_{k=0}^{K-1} (l_i^{(k)} - \bar{l}_i)^2. \quad (16)$$

Данная функция, которая представляет собой зависимость величины дисперсии от времени, имеет в дискретном случае область определения, состоящую из N точек, а значит, может быть интерпретирована как конечный вектор длины N в нормированном пространстве [6]. Это дает возможность использовать инструменты, применяемые к векторам, для получения их характеристик. В текущей ситуации это позволяет оценить величину общей дисперсии, используя какую-либо норму вектора.

Для оценки вполне подойдет норма L^1 (манхэттенское расстояние):

$$|D| = \sum_{i=0}^{N-1} |D_i|. \quad (17)$$

Однако здесь прослеживается зависимость от N , выражающаяся в том, что чем больше точек, тем больше будет эта величина. Поэтому есть смысл сравнивать функции только с одинаковым числом точек. Но при изменении числа точек все имеющиеся данные необходимо повторно пересчитывать.

Для большей резистентности к разбиению можно ввести следующий вектор дисперсии:

$$\tilde{D} = \langle \frac{D_0}{N}, \frac{D_1}{N}, \dots, \frac{D_{N-1}}{N} \rangle. \quad (18)$$

Тогда его норма:

$$\tilde{\sigma} = |\tilde{D}| = \sum_{i=0}^{N-1} |\tilde{D}_i|. \quad (19)$$

Среднеквадратичное отклонение:

$$\sigma = \sqrt{|D|}, \quad (20)$$

или

$$\tilde{\sigma} = \sqrt{|\tilde{D}|}. \quad (21)$$

Другой способ сравнений – на основе общего времени. Поскольку изначально, до предобработки, подпись представлена точками в моменты времени $\{t_i\}_{j=1}^{M-1}$, где M – общее количество зафиксированных точек до предобработки, то для вычисления общего затраченного времени достаточно найти разность между последней временной меткой и первой:

$$dt = t_{M-1} - t_0, \text{ считая, что } t_{M-1} > t_0. \quad (22)$$

Пусть для каждой из K подписей было вычислено затраченное на ее написание время – $\{dt_j\}_{j=0}^{K-1}$. Тогда среднее время будет выражаться формулой:

$$\overline{dt} = \frac{1}{N} \sum_{j=0}^{K-1} dt_j. \quad (23)$$

Дисперсия будет иметь вид:

$$D_t = \frac{1}{N} \sum_{j=0}^{K-1} (dt_j - \overline{dt})^2. \quad (24)$$

Еще один признак – общая длина подписи как геометрической кривой. Стоит отметить, что при вычислении на необработанных данных данный признак очень подвержен влиянию размера экрана, что сильно снижает его ценность. Поэтому более правильным вариантом будет использовать не саму длину, полученную на исходных данных, а ее отношение к диагонали экрана [7]. Также для вычисления можно использовать точки, полученные после предобработки, когда диапазон изменения координат будет лежать на отрезке от 0 до 1, но подобный подход может сильно потерять в точности из-за полного отбрасывания информации о занимаемой области подписи на экране.

Пусть подпись состоит из N точек с координатами $x_i, y_i, i = \overline{0..N-1}$.

Тогда ее длина l будет выражаться длиной ломанной:

$$l = \sum_{i=0}^{N-2} \sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}. \quad (25)$$

Если имеется K подписей с длинами $\{l_i\}_{i=0}^{K-1}$, то среднее значение будет:

$$\bar{l} = \frac{1}{K} \sum_{i=0}^{K-1} l_i. \quad (26)$$

В данном варианте дисперсия имеет вид:

$$D_t = \frac{1}{K} \sum_{i=0}^{K-1} (l_i - \bar{l})^2. \quad (27)$$

Результаты и обсуждение

Для определения эффективности алгоритмов на имеющихся данных часто используют ошибки I и II рода.

Ошибка первого рода, или «ложноположительная ошибка», происходит, когда алгоритм верификации неправильно классифицирует подлинную подпись как поддельную. Это может быть особенно проблематично, поскольку такой результат может создать недоверие к пользователю, который пытается подтвердить свою личность.

Ошибка второго рода, также известная как «ложноотрицательная ошибка», происходит, когда алгоритм верификации неправильно классифицирует поддельную подпись как подлинную. В контексте верификации рукописной подписи это может произойти, если система, анализируя параметры подписи (например, скорость написания, длину, давление на бумагу и т. д.), ошибочно принимает подделку за оригинал, давление на бумагу и т. д.), ошибочно принимает подделку за оригинал. В данной работе исследование проводилось только по отношению к ошибкам второго рода [8].

Данные методы имеют некоторые преимущества по сравнению с другими способами выделения признаков, также как и недостатки. К преимуществам можно отнести то, что разные люди имеют различную скорость написания текста, как и своей подписи, что сказывается на общем затраченном времени ее написания. Также каждый человек имеет свои индивидуальные особенности написания всевозможных форм и

частей кривой подписи, что может служить признаком для определения ее автора. Кроме того, вычисление некоторых из представленных признаков не требует сколько-нибудь значимых ресурсов и может выполняться даже на слабых вычислительных устройствах. Например, чтобы вычислить затраченное на написание полное время, достаточно из временной метки последней точки вычесть временную метку начальной точки.

Необходимо отметить, что кроме преимуществ данные подходы имеют и недостатки. К ним можно отнести то, что параметры подписи могут варьироваться в зависимости от условий написания и состояния человека в момент написания [9]. К таким проблемам относятся усталость, настроение или физические ограничения (например, травмы руки). Данные обстоятельства могут привести к ложным срабатываниям и снижению точности аутентификации. При этом сам способ аутентификации на основании рукописной подписи подвержен влиянию перечисленных условий, поэтому данные ограничения не являются особенными для представленных в статье подходов.

Заключение

В данной статье были рассмотрены подходы к аутентификации пользователей, основанные на анализе длины и временных параметров рукописной подписи. Большое внимание было уделено разработке функции, описывающей зависимость длины подписи от времени, а также способу сравнения этих функций. Данный подход открывает новые горизонты в области биометрической аутентификации, позволяя использовать временные характеристики как дополнительные признаки для повышения точности аутентификации.

В процессе анализа были представлены методы поточечного сравнения функций длины и их производных. Производная длины подписи по времени представляет собой важный индикатор, так как показывает, как изменяется скорость написания в разные моменты времени [10]. Такой анализ может помочь в выявлении аномалий, которые могут указывать на попытку подделки подписи, а также на индивидуальные особенности подписи в каждом из интервалов ее написания, что делает систему аутентификации более надежной.

Кроме того, были рассмотрены такие признаки, как полное затраченное время на написание подписи и полная длина подписи. Эти параметры могут служить дополнительными критериями для аутентификации, каждый человек имеет свои уникальные временные паттерны в процессе их написания, а также они не требуют затратных вычислительных операций, что делает доступным их использование на широком ряде самых разнообразных устройств [11].

Были представлены способы вычисления усредненных значений указанных признаков для множества подписей, а также способ определения отклонения от этих значений. Это отклонение часто используется для выбора порога, показывающего, насколько новая подпись находится близко к значению «в среднем» по выбранным признакам. Правильный выбор порогового значения диктуется условиями применения подписи, что характеризуется соотношением риска принятия поддельной подписи к отбрасыванию истинной.

Важным аспектом работы стало представление способов оценки качества алгоритмов аутентификации на основе использования ошибок первого и второго рода. Ошибка первого рода подразумевает неверное отклонение истинной подписи, в то время как ошибка второго рода связана с неверным принятием подделки за оригинал. Анализ данных ошибок позволяет оценить надежность и точность предложенных методов, а также выявить области, требующие дальнейшего улучшения [12].

В заключение, аутентификация на основе анализа длины и временных параметров рукописной подписи представляет собой перспективное направление в области биометрической идентификации. Представленные методы и подходы могут повысить уровень безопасности систем аутентификации пользователей, выделяя довольно специфические признаки для анализа. Дальнейшие исследования в этой области могут привести к созданию более эффективных и надежных алгоритмов, способных адаптироваться к индивидуальным особенностям пользователей по выбранным аспектам и минимизировать риски, связанные с подделкой рукописной подписи.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Мискевич П.Л., Петровец В.Н., Раловец А.А. Развитие и оценка нейросетевых методов верификации собственноручной подписи. В сборнике: *Компьютерные системы и сети: сборник статей 59-й научной конференции аспирантов, магистрантов и студентов, 17–21 апреля 2023 года, Минск, Беларусь*. Минск: Белорусский государственный университет информатики и радиоэлектроники; 2023. С. 365–369.
Miskevich P.L., Petrovets V.N., Ralovets A.A. Development and Evaluation of Neural Network Methods for Handwritten Signature Verification. In: *Komp'yuternye sistemy i seti: sbornik statei 59-i nauchnoi konferentsii aspirantov, magistrantov i studentov, 17–21 April 2023, Minsk, Belarus*. Minsk: Belarusian State University of Informatics and Radioelectronics; 2023. P. 365–369. (In Russ.).
2. Xiao W., Wu H. Learning Features for Offline Handwritten Signature Verification Using Spatial Transformer Network. *Scientific Reports*. 2025;15. <https://doi.org/10.1038/s41598-025-92704-3>
3. Козловский В.А., Максимова А.Ю. Алгоритм распознавания, основанный на нечетком подходе. *Искусственный интеллект*. 2008;(4):594–599.
4. Левинский А.Т. Алгоритмы верификации рукописных подписей на основе нейронных сетей. *StudNet*. 2020;3(3):395–402.
Levinsky A.T. Manual Signature Verification Algorithms Based on Neural Networks. *StudNet*. 2020;3(3):395–402. (In Russ.).
5. Иванов Ю.С., Авдеенко А.А. Обзор метода верификации личности по подписи и разработка программного обеспечения. *Вестник научного общества студентов, аспирантов и молодых ученых*. 2014;(1):3–8.
6. Хаерова Э.И. Использование нейросетевых технологий для идентификации рукописной подписи человека. В сборнике: *Нигматуллинские чтения – 2023: сборник докладов Международной научной конференции, 09–12 октября 2023 года, Казань, Россия*. Казань: Изд-во АН РТ; 2023. С. 428–431.
Haerova E.I. Using Neural Network Technologies to Identify A Person's Signature. In: *Nigmatullin's Readings – 2023: Proceedings of the International Conference, 09–12 October 2023, Kazan, Russia*. Kazan: TAS Publishing House; 2023. P. 428–431. (In Russ.).
7. Кадильников Т.М., Минюк О.Н. Математическое моделирование процессов верификации в документообороте организации. В сборнике: *Банковская система: устойчивость и перспективы развития: сборник научных статей X Международной научно-практической конференции по вопросам финансовой и банковской экономики, посвященной 75-летию банковского образования на белорусском Полесье, 25 октября 2019 года, Пинск, Беларусь*. Пинск: Полесский государственный университет; 2019. С. 321–326.

8. Дробинцев П.Д., Сергеев Д.И., Воинов Н.В. Система онлайн верификации подписей для мобильных устройств с многоуровневым датчиком давления. В сборнике: *XX Международная конференция по мягким вычислениям и измерениям (SCM'2017): Том 1, 24–26 мая 2017 года, Санкт-Петербург, Россия*. Санкт-Петербург: Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина); 2017. С. 520–522.
Drobintsev P.D., Sergeev D.I., Voinov N.V. Online Signature Verification System for Mobile Devices with Multilevel Pressure Sensor. In: *The XX International Conference on Soft Computing and Measurements (SCM'2017): Volume 1, 24–26 May 2017, Saint Petersburg, Russia*. Saint Petersburg: Saint Petersburg Electrotechnical University "LETI"; 2017. P. 520–522. (In Russ.).
9. Анисимова Э.С., Аникин И.В. Сравнительный анализ нейросетевых моделей для распознавания динамики рукописных подписей. *Электроника, фотоника и киберфизические системы*. 2024;4(3):77–85.
Anisimova E.S., Anikin I.V. Comparative Analysis of Neural Network Models for Handwritten Signature Dynamics Recognition. *Electronics, Photonics and Cyber-Physical Systems*. 2024;4(3):77–85. (In Russ.).
10. Старовойтов В.В. Следует ли нормализовать данные динамических подписей перед верификацией методом DTW? В сборнике: *Big Data и анализ высокого уровня: сборник научных статей X Международной научно-практической конференции: Часть 2, 13 марта 2024 года, Минск, Беларусь*. Минск: Белорусский государственный университет информатики и радиоэлектроники; 2024. С. 391–400.
Starovoitov V.V. Should We Normalize Dynamic Signatures Data Before DTW-Based Verification? In: *Big Data and Advanced Analytics: sbornik nauchnykh statei X Mezhdunarodnoi nauchno-prakticheskoi konferentsii: Part 2, 13 March 2024, Minsk, Belarus*. Minsk: Belarusian State University of Informatics and Radioelectronics; 2024. P. 391–400. (In Russ.).
11. Maergner P., Pondenkandath V., Alberti M., et al. Offline Signature Verification by Combining Graph Edit Distance and Triplet Networks. In: *Structural, Syntactic, and Statistical Pattern Recognition: Joint IAPR International Workshop, S+SSPR 2018: Proceedings, 17–19 August 2018, Beijing, China*. Cham: Springer; 2018. P. 470–480.
https://doi.org/10.1007/978-3-319-97785-0_45
12. Кузнецов В.В. Использование матрицы углов для повышения точности метода биометрической верификации по динамической подписи. *Техника и технология: новые перспективы развития*. 2014;(XV):72–75.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Дзямко-Гамулец Роман Николаевич, магистр, студент факультета кибернетики и информационной безопасности, Московский технический университет связи и информатики, Москва, Российская Федерация.
e-mail: roman.dzyamko-gamulets@outlook.com

Roman N. Dzyamko-Gamulets, master, student of Cybernetics and Information Security Faculty, Moscow Technical University of Communications and Informatics, Moscow, the Russian Federation.

Иевлев Олег Павлович, кандидат технических наук, декан факультета кибернетики и информационной безопасности, Московский технический университет связи и информатики, Москва, Российская Федерация.
e-mail: ievlev@mtuci.ru

Oleg P. Ievlev, Candidate of Engineering Sciences, Dean of the Cybernetics and Information Security Faculty, Moscow Technical University of Communications and Informatics, Moscow, the Russian Federation.

*Статья поступила в редакцию 03.05.2025; одобрена после рецензирования 29.05.2025;
принята к публикации 06.06.2025.*

*The article was submitted 03.05.2025; approved after reviewing 29.05.2025;
accepted for publication 06.06.2025.*