

17. Sugeno M., Yasukawa T. A fuzzy-logic-based approach to qualitative modeling, *IEEE Trans. on Fuzzy Systems*, 1993, Vol. 1, pp. 7-31.
18. Mamdani E.H. Application of fuzzy algorithms for control of a simple dynamic plant, *Proc. Inst. Elect. Eng.*, 1974, Vol. 121, pp. 1585-1588.
19. Klement E., Mesiar R., and Pap E. *Triangular Norms (Trends in Logic 8)*. Kluwer Academic Publishers, Dordrecht 2000.
20. Ruspini E.H. A new approach to clustering, *Inform. and Control*, 1969, Vol. 15, pp. 22-32.
21. Zadeh L.A. The concept of a linguistic variable and its application to approximate reasoning I, *Inform. Sci.*, 1975, No. 8, pp. 199-250.
22. Zadeh L.A. The concept of a linguistic variable and its application to approximate reasoning II, *Inform. Sci.*, 1975, No. 8, pp. 301-357.
23. Zadeh L.A. The concept of a linguistic variable and its application to approximate reasoning III, *Inform. Sci.*, 1975, No. 9, pp. 43-80.
24. Kovalev S.M., Tarassov V.B., Dolgiy A.I., Dolgiy I.D., Koroleva M.N., Khatlamadzhiyan A.E. Intelligent Measurement in Railcar On-Line Monitoring: From Measurement Ontologies to Hybrid Information Granulation System, *Proceedings of the Second International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'17)*, 2017, Vol. 1, pp. 169-181.

Статью рекомендовал к опубликованию д.т.н., профессор А.В. Боженюк.

Ковалев Сергей Михайлович – Центр Интеллектуальных технологий Ростовского филиала АО «НИИАС»; e-mail: ksm@rfniias.ru; 344038, г. Ростов-на-Дону, ул. Ленина, 44/13; начальник; д.т.н.; профессор РГУПС.

Долгий Александр Игоревич – e-mail: adolgy@list.ru; первый заместитель директора; к.т.н.; доцент РГУПС.

Kovalev Sergey Mikhailovich – Intellectual Technologies Center of Rostov Branch of JSC "NIAS"; e-mail: ksm@rfniias.ru; 44/13, Lenin street, Rostov-on-don, 344038, Russia; head; dr. of eng. sc.; professor of RGUPS.

Dolgy Alexander Igorevich – e-mail: adolgy@list.ru; first deputy director; cand. of eng. sc.; associate professor of the RSTU.

УДК 004.067

DOI 10.23683/2311-3103-2018-5-142-151

Ю.А. Брюхомицкий

ТЕКСТОНЕЗАВИСИМАЯ ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ ПО ДИНАМИЧЕСКИМ БИОМЕТРИЧЕСКИМ ПАРАМЕТРАМ НА ОСНОВЕ ИММУННОЙ МОДЕЛИ КЛОНАЛЬНОЙ СЕЛЕКЦИИ

Предлагается иммунологический подход к решению задачи распознавания сигналов динамической биометрии, базирующийся на принципах массово-параллельной децентрализованной обработки данных, использующихся в искусственных иммунных системах. Особенностью подхода является представление сигналов динамической биометрии последовательностями информационных единиц определенного формата, с последующей обработкой в темпе их поступления на основе иммунологической модели клональной селекции с положительным отбором. В качестве информационных единиц выступают синтаксически связанные фрагменты текста соответствующей модальности, которые представлены многомерными векторами в рабочем пространстве признаков. В фазе обучения создается начальная популяция детекторов в метрике векторов исследуемой последовательности биометрических данных. Затем по принципу положительного отбора выявляются детекторы начальной популяции, которые в пространстве признаков наиболее близки к областям распределения соответствующих биометрических данных. Близость векторов в пространстве признаков моделирует

свойство аффинности клеток иммунной системы. Выявленные детекторы на основе итерационной процедуры подвергаются клонированию, гипермутации и отбора и в конечном итоге образуют популяцию детекторов иммунной памяти. Останов процедуры обучения осуществляется при достижении заданного максимального размера популяции детекторов иммунной памяти. В фазе распознавания элементы анализируемой биометрической последовательности данных сопоставляются с детекторами популяции памяти с использованием меры близости Евклида. Критический уровень близости определяет границу для принятия системой решения «свой/чужой» и задается, исходя из допустимых ошибок первого рода. Для принятия системой решения «свой» – «чужой» используется статистический подход, при котором контролируется частота выполнения условия критической близости, определяющая статистическую вероятность принадлежности анализируемой биометрии «чужо-му». Предлагаемый подход в рамках иммунологического представления позволяет обобщить существенно различные методы идентификации личности по динамическим биометрическим параметрам разной модальности. Положительными отличиями предлагаемого подхода являются: возможность текстонезависимого анализа динамической биометрии любой модальности, произвольного объема и содержания; непрерывная оценка принадлежности биометрических данных в темпе их поступления, с возможностью своевременного принятия решения о присутствии «чужого»; применение иммунологической модели, которая хорошо согласуется с большинством задач динамической идентификации личности, что позволяет существенно уменьшить число детекторов, необходимых для эффективной идентификации личности.

Текстонезависимая идентификация личности; динамическая биометрия; искусственные иммунные системы; векторное представление данных; иммунная модель клональной селекции.

Yu.A. Bryuhomitsky

TEXT-INDEPENDENT PERSONALITY IDENTIFICATION WITH THE USE OF DYNAMIC BIOMETRIC PARAMETERS BASED ON THE IMMUNE MODEL OF CLONAL SELECTION

An immunological approach is proposed to solve the problem of recognition of dynamic biometric signals, based on the principles of massively parallel decentralized data processing used in artificial immune systems. A special feature of approach is presentation of dynamic biometrics signals by sequences of informational units of a certain format, with their following RTP processing on the basis of the immunological clonal selection model with positive selection. As an informational units are syntactically related fragments of the text of the corresponding modality. They are represented by multidimensional vectors in the workspace of features. In the training phase, an initial population of detectors is created in the metric of the vectors of the investigated sequence of biometric data. Then, according to the principle of positive selection, the detectors of the initial population are identified, which in the feature space are closest to the areas of distribution of the corresponding biometric data. The proximity of the vectors in the feature space models the property of the affinity of the immune system cells. Revealed detectors, using the iterative procedure, are subjected to cloning, hypermutation and selection and ultimately form a population of immune memory detectors. The training procedure is stopped when the specified maximum size of the population of the immune memory detectors is reached. In the recognition phase, the elements of the analyzed biometric data sequence are compared with the memory population detectors using the Euclid proximity measure. The critical level of proximity defines the boundary for the decision "well-known/stranger" making by the system and is specified based on the permissible errors of the first kind. To identify "well-known/stranger", a statistical approach is used, in which the frequency of the critical proximity condition is controlled, which determines the statistical probability of belonging to the analyzed biometry to "stranger". The proposed approach within the framework of the immunological presentation allows to generalize essentially different methods of personality identification by the dynamic biometric parameters of different modalities. The positive differences of the proposed approach are: the possibility of text-independent analysis of dy-

dynamic biometrics of any modality, arbitrary volume and content; continuous assessment of the biometric data in RTP with the possibility of timely decision-making on the presence of "stranger"; the use of an immunological model that fits well with most of the tasks of dynamic personality identification, which allows to reduce significantly the number of detectors required for effective identification of a person.

Text-independent personality identification; dynamic biometry; artificial immune systems; vector data representation; immune model of clonal selection.

Введение. В информационной безопасности все большее распространение получают динамические системы биометрической идентификации личности (динамическая биометрия), которые основаны на анализе индивидуальных особенностей хорошо заученных подсознательных движений человека. Практическое применение в настоящее время получили системы анализа голоса [1–3], рукописи [4–8] и клавиатурного почерка [9–12]. Динамическая биометрия используется преимущественно как средство аутентификации личности при входе в компьютерные и мобильные системы, а также для удаленной (голосовой) аутентификации.

Динамические системы биометрической идентификации делятся на текстозависимые и текстонезависимые. Первые – менее сложны в реализации, но весьма уязвимы для атак воспроизведения записанного текста. Вторые обеспечивают идентификацию личности при воспроизведении ею любого текста на любом языке, но существенно сложнее в реализации и требуют больше времени для проведения процедуры идентификации. Вместе с тем использование текстонезависимой биометрической идентификации позволяет существенно более широкий круг задач информационной безопасности таких как: проведение непрерывной скрытной верификации работающих пользователей компьютерных систем (клавиатурная биометрия); скрытное выявление инсайдеров (клавиатурная биометрия); скрытное выявление психофизических отклонений личности от нормативного (голосовая, рукописная и клавиатурная биометрия); аудит безопасности компьютерных систем на основе интерактивного взаимодействия с пользователями (аналог детектора лжи) (голосовая, рукописная и клавиатурная биометрия) и др.

В текстонезависимой динамической биометрии эталоны личности строятся на основе достаточно больших образцов текста соответствующей модальности. При этом возникает ряд принципиальных проблем, связанных с необходимостью использования биометрических эталонов большой размерности, трудностью их формирования, анализа и сопоставления с образцами динамической биометрии.

Постановка задачи. Общей особенностью текстонезависимой динамической биометрии является представление исходных данных сигналами (функциями времени) структура которых содержит все необходимые для идентификации индивидуальные особенности личности. Для решения задачи распознавания таких сигналов предложено множество методов, которые сводятся к переводу их в какое-либо статическое представление в частотной, частотно-временной или временной областях. После чего задача распознавания биометрических образов решается в формате их статического представления.

В данной работе предлагается подход к решению задачи распознавания сигналов динамической биометрии, базирующийся на принципах массово-параллельной децентрализованной обработки данных, используемых в искусственных иммунных системах (ИИС) [13–15].

Особенностью подхода является представление сигналов динамической биометрии в виде последовательности информационных иммунологических единиц определенного формата, с последующей децентрализованной обработкой в темпе их поступления на основе определенной иммунологической модели ИИС. Такое представление и обработка имитируют массово-параллельный обмен информацией на уровне клеток, наблюдаемую в живой иммунной системе.

Встает вопрос какую иммунологическую модель лучше использовать для решения поставленной задачи. Наибольшее распространение в ИИС получили две модели модель отрицательного отбора (МОО) [16–18] и модель клональной селекции (МКС) [19–20]. МОО – более эффективна в том случае, когда область «чужие» существенно меньше области «свои». МКС, напротив, более эффективна в том случае, когда область «свои» существенно меньше области «чужие».

Для задач распознавания образов динамической биометрии при использовании режима верификации (разделение данных только на 2 класса: «свой» и «чужие»), очевидно, больше подходит МКС. Число детекторов, необходимых для эффективного распознавания биометрических данных одного конкретного класса «свой» по отношению к биометрическим данным многочисленных «чужих» в этом случае будет существенно меньше, чем при использовании МОО.

МКС можно строить по двум принципам: с положительным или отрицательным отбором. В первом случае детекторы представляют образцы класса «свой», во втором – образцы класса «чужие». Поскольку в задачах верификации образов динамической биометрии класс «свой» существенно меньше класса «чужие», то оптимальным вариантом будет МКС с положительным отбором, для которой потребное количество детекторов будет меньше.

В результате, для решения задач распознавания образов динамической биометрии с использованием режима верификации как потенциально более эффективная выбрана МКС с положительным отбором.

Решение поставленной задачи. Воспроизведение произвольного текста средствами динамической биометрии любой модальности реализуется совокупностью заученных подсознательных движений, которые преобразуются в электрические сигналы (функции времени) В общем случае эти сигналы являются многомерными: $x(t) = x_1(t), x_2(t), \dots, x_n(t)$.

На этапе предварительной обработки сигнал $x(t)$ оцифровывается $x(t) \rightarrow x(t_i) = x(i)$, $i = 1, 2, \dots$, масштабируется, из него исключаются длительные паузы, не обусловленные индивидуальными особенностями воспроизведения текста. В голосовой биометрии исключаются также неинформативные (с точки зрения распознавания голоса) фонемы шипящих звуков.

Отсчеты сигнала $x(i)$, $i = 1, 2, \dots$ можно рассматривать как точки метрического пространства E^n , представленные векторами признаков $x_i = x_{1i}, x_{2i}, \dots, x_{ni}$, а сам сигнал $x(i)$, – как последовательность $X_i = x_1, x_2, \dots$ элементов, представленных векторами признаков: x_i . В математическом смысле последовательность X_i «пробегает» конечное множество Ψ_x векторов признаков x_i биометрии данной личности.

Исследования в области динамической биометрии [12, 21], показывают, что индивидуальные особенности личности в наибольшей степени проявляются при воспроизведении не одиночных символов текста, а синтаксически связанных фрагментов текста. Использование этого феномена при анализе позволяет строить системы биометрической идентификации личности с существенно более высокими характеристиками по точности.

Следуя указанному подходу последовательность X_i расчленяется на фрагменты одинакового размера по r отсчетов x_i в каждом фрагменте. Результатом будет новая последовательность $Y_j = y_1, y_2, \dots$, $j = 1, 2, \dots$, каждый элемент y_j которой содержит r n -мерных векторов x_i исходной последовательности X_i :

$$y_j = x_1, x_2, \dots, x_r, \quad i = 1, 2, \dots, r, \quad j = 1, 2, \dots$$

Совокупность векторов x_1, x_2, \dots, x_r каждого фрагмента y_j можно представить как один s -мерный вектор y_j , содержащий $s = n \times r$ компонент:

$$\mathbf{y}_j = \begin{bmatrix} y_{11} & y_{12} & \dots & y_{1r} \\ y_{21} & y_{22} & \dots & y_{2r} \\ \dots & \dots & \dots & \dots \\ y_{n1} & y_{n2} & \dots & y_{nr} \end{bmatrix}.$$

В итоге, образ динамической биометрии личности будет представлен последовательностью \mathbf{Y}_j s -мерных векторов признаков \mathbf{y}_j в пространстве признаков E^s .

Последовательность \mathbf{Y}_j , ограниченная N_y элементами

$$\bar{\mathbf{Y}}_j = \mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_{N_y}, \quad j = 1, 2, \dots, N_y,$$

можно трактовать как биометрический эталон данной личности. При распознавании данных ДБ в режиме верификации последовательность $\bar{\mathbf{Y}}_j$, выступает в качестве эталона «своего». При этом каждая информационная единица \mathbf{y}_j последовательности $\bar{\mathbf{Y}}_j$ отражает представление нескольких последовательно воспроизводимых (голосом, клавиатурой или ГП) символов текста. Общий характер распределения биометрических данных определенной личности представлен множеством областей, каждая из которых отражает распределение одного определенного фрагмента \mathbf{y}_j контекстно-связанных символов. Число областей соответствует числу типов фрагментов \mathbf{y}_j , встречающихся в эталонной последовательности $\bar{\mathbf{Y}}_j$.

Предлагаемый принцип текстонезависимой идентификации личности по биометрическим параметрам основан на использовании модели МКС ИИС [18–19] и заключается в следующем.

В фазе обучения ИИС создается начальная популяция детекторов в метрике векторов \mathbf{y}_j . Затем по принципу положительного отбора выявляются детекторы начальной популяции, которые в пространстве E^s наиболее близки к областям распределения векторов \mathbf{y}_j . Близость векторов в пространстве E^s моделирует свойство аффинности клеток иммунной системы. Выявленные детекторы на основе итерационной процедуры подвергаются клонированию, гипермутации и отбора. Останов процедуры обучения осуществляется по определенным признакам, свидетельствующим о достижении достаточной степени покрытия детекторами области распределения биометрических признаков в рабочем пространстве E^s .

На этапе распознавания контролируемые биометрические данные личности \mathbf{Y}_j сравниваются с детекторами по принципу близости. Соотношение числа срабатывающих детекторов к их общему числу дает оценку вероятности для принятия системной решения «свой–чужой».

Алгоритм обучения ИИС.

1. Создание последовательности $\bar{\mathbf{Y}}_j$, $j = 1, 2, \dots, N_y$, представляющей биометрический эталон «своего».

2. Создание путем случайной генерации (с равномерным законом распределения) начальной популяции детекторов $\mathbf{D}_k^\lambda = \mathbf{d}_1, \mathbf{d}_2, \dots, \mathbf{d}_{N_d}$, $\lambda = 0$, $k = 1, 2, \dots, N_d$ представленных векторами в формате векторов \mathbf{y}_j .

3. Для каждой пары $\mathbf{d}_k \in \mathbf{D}_k^\lambda$ и $\mathbf{y}_j \in \bar{\mathbf{Y}}_j$ вычисляется степень их взаимной аффинности. В качестве меры аффинности a_{kj} используется Евклидово расстояние между векторами \mathbf{d}_k и \mathbf{y}_j :

$$a_{kj}(\mathbf{d}_k, \mathbf{y}_j) = \sqrt{\sum_{p=1}^N (d_{kp} - y_{jp})^2}, \quad p = 1, 2, \dots, N, \quad N = N_d \cdot N_y.$$

Результатом вычислений будет матрица взаимной аффинности \mathbf{A} , содержащая $N = N_d \cdot N_y$ элементов a_{kj} :

$$\mathbf{A} \| a_{kj}(\mathbf{d}_k, \mathbf{y}_j) \| = \left\| \begin{array}{cccc} a_{11} & a_{12} & \dots & a_{1N_y} \\ a_{21} & a_{22} & \dots & a_{2N_y} \\ \dots & \dots & \dots & \dots \\ a_{N_d 1} & a_{N_d 2} & \dots & a_{N_d N_y} \end{array} \right\|, \\ k = 1, 2, \dots, N_d \quad j = 1, 2, \dots, N_y.$$

4. Из каждого столбца матрицы \mathbf{A} отбирается l из N_d детекторов \mathbf{d}_k , соответствующих наибольшей взаимной аффинности $a_{kj}(\mathbf{d}_k, \mathbf{y}_j)$, $k = 1, 2, \dots, l$, $j = 1, 2, \dots, N_y$ и подвергаются операции клонирования C :

$$C[\mathbf{d}_k] = \mathbf{d}_k^c, \quad k = 1, 2, \dots, l \quad c = 1, 2, \dots, q.$$

Количество образуемых клонов q_k каждого из l детекторов \mathbf{d}_k^c пропорционально взаимной аффинности $a_{kj}(\mathbf{d}_k, \mathbf{y}_j)$:

$$q_k \propto k_c \cdot a_{kj}(\mathbf{d}_k, \mathbf{y}_j),$$

где k_c коэффициент пропорциональности при клонировании.

При этом общее количество образованных клонов должно оставаться равным N_d :

$$\sum_{k=1}^l q_k = \left[\sum_{k=1}^l k_c \cdot a_{kj}(\mathbf{d}_k, \mathbf{y}_j) \right] = N_d.$$

То есть все детекторы популяции \mathbf{D}_k^λ заменяются клоном \mathbf{d}_k^c : $\mathbf{D}_k^\lambda \rightarrow \mathbf{D}_k^{\lambda c}$. Очевидно, что для выполнения этого условия

$$k_c = N_d / \sum_{k=1}^l a_{kj}(\mathbf{d}_k, \mathbf{y}_j).$$

Операция клонирования повышает вероятность покрытия детекторами областей распределения соответствующих биометрических признаков \mathbf{y}_j .

5. Все клоны \mathbf{d}_k^c популяции $\mathbf{D}_k^{\lambda c}$ подвергаются операции гипермутации G :

$$G[\mathbf{d}_k^c] = \mathbf{d}_k^{cG}, \quad k = 1, 2, \dots, l \quad c = 1, 2, \dots, q.$$

Операцию гипермутации G клонов предлагается реализовать путем изменения на случайные величины $0 < \xi < \delta$ некоторого числа m компонент векторов детекторов \mathbf{d}_k^c . При этом гипермутация G клонов \mathbf{d}_k^c осуществляется обратно пропорционально взаимной аффинности $a_{kj}(\mathbf{d}_k, \mathbf{y}_j)$:

$$G \propto k_m / a_{kj}(\mathbf{d}_k, \mathbf{y}_j),$$

где k_m – коэффициент гипермутации клонов \mathbf{d}_k^{cG} определяемый из условия: $m = 1$ при $\max_{k=1,2,\dots,l} a_{kj}(\mathbf{d}_k, \mathbf{y}_j)$

Операция гипермутации сужает область поиска новых эффективных детекторов.

Детекторы \mathbf{d}_k^{cGm} заменяют популяцию $\mathbf{D}_k^{\lambda c}$ на новую $\mathbf{D}_k^{\lambda cG}$.

6. Для каждой пары $\mathbf{d}_k^{cG} \in \mathbf{D}_k^{\lambda cG}$ и $\mathbf{y}_j \in \bar{\mathbf{Y}}_j$ вычисляется степень взаимной аффинности.

$$a_{kj}(\mathbf{d}_k^{cG}, \mathbf{y}_j) = \sqrt{\sum_{p=1}^N (d_{kp}^{cG} - y_{jp})^2}, \quad p = 1, 2, \dots, N.$$

Результатом будет матрица взаимной аффинности \mathbf{A} , содержащая $N = N_d \cdot N_y$ элементов a_{ij} :

$$\mathbf{A} \| a_{kj}(\mathbf{d}_k^{cG}, \mathbf{y}_j) \|, \quad k = 1, 2, \dots, N_d \quad j = 1, 2, \dots, N_y.$$

7. Из каждого столбца матрицы \mathbf{A} отбирается совокупность из l детекторов \mathbf{d}_k^{CG} , соответствующих наибольшей взаимной аффинности $a_{kj}(\mathbf{d}_k^{CG}, \mathbf{y}_j)$, $k = 1, 2, \dots, l$, $j = 1, 2, \dots, N_y$. Полученные детекторы \mathbf{d}_k^{CGm} образуют популяцию детекторов памяти \mathbf{D}^M .

8. Проверка условия останова: при невыполнении условия, – переход на следующий шаг, иначе на шаг 10.

9. $(N_d - l)$ детекторов популяции $\mathbf{D}_k^{\lambda CG}$, обладающих наименьшей аффинностью $a_{kj}(\mathbf{d}_k, \mathbf{y}_j)$ заменяются новыми, путем их случайной генерации (с равномерным законом распределения) новой популяции детекторов $\mathbf{D}_k^\lambda = \mathbf{d}_1, \mathbf{d}_2, \dots, \mathbf{d}_{N_d}$, $\lambda = \lambda + 1$, $k = 1, 2, \dots, (N_d - l)$ представленных векторами в формате векторов \mathbf{y}_j .

10. Останов, конец алгоритма.

Условием останова алгоритма является достижение заданного максимального размера популяции детекторов памяти $\mathbf{D}^M = \mathbf{D}_{\max}^M$, образующейся при $k = N_M$.

В фазе распознавания элементы \mathbf{y}_j анализируемой последовательности биометрических признаков \mathbf{Y}_j сопоставляются с детекторами \mathbf{d}_k^M популяции памяти \mathbf{D}^M , $k = 1, 2, \dots, N_M$ с использованием меры близости Евклида между векторами \mathbf{y}_j и \mathbf{d}_k^M :

$$\nabla(\mathbf{y}_j, \mathbf{d}_k^M) = \sqrt{\sum_{v=1}^s (y_{jv} - d_{kv})^2}.$$

Критический уровень близости $\nabla(\mathbf{y}_j, \mathbf{d}_k^M) = \nabla^*$ определяет границу для принятия системой решения «свой/чужой» и задается, исходя из допустимых ошибок первого рода. Если для некоторой пары \mathbf{y}_j и \mathbf{d}_k^M $\nabla(\mathbf{y}_j, \mathbf{d}_k^M) > \nabla^*$, то считается, что элемент \mathbf{y}_j анализируемой биометрии \mathbf{Y}_j , принадлежит «чужому».

Существенные вариации параметров динамической биометрии в последовательностях \mathbf{Y}_j и значительные размеры самих последовательностей \mathbf{Y}_j определяют целесообразность применения статистического подхода для принятия ИИС решения «свой»-«чужой» [22, 23]. При таком подходе контролируется частота f выполнения условия $\nabla(\mathbf{y}_j, \mathbf{d}_k^M) > \nabla^*$, которая определяет статистическую вероятность принадлежности анализируемой биометрии «чужому»:

$$\hat{P}^{\text{ч}} \approx f = n_{\nabla^*}^+ / n_{\nabla},$$

где $n_{\nabla^*}^+$ – число случаев выполнения условия $\nabla(\mathbf{y}_j, \mathbf{d}_k^M) > \nabla^*$ в n_{∇} проведенных операциях сопоставлений \mathbf{y}_j с \mathbf{d}_k^M .

Принятие решения о принадлежности анализируемой биометрии «чужому» считается обоснованным, при превышении частоты f заданного порогового значения $f_{\text{п}}$:

$$\mathbf{Y}_j \equiv \begin{cases} \mathbf{Y}_j^{\text{с}}, & \text{если } f < f_{\text{п}}; \\ \mathbf{Y}_j^{\text{ч}}, & \text{если } f \geq f_{\text{п}}, \end{cases}$$

где $\mathbf{Y}_j^{\text{с}}$ – последовательность биометрических признаков «своего»;

$\mathbf{Y}_j^{\text{ч}}$ – последовательность векторов признаков «чужого»;

Заключение. Предлагаемый подход в рамках иммунологического представления позволяет обобщить существенно различные существующие методы идентификации личности по динамическим биометрическим параметрам разной модальности – голоса, рукописи и клавиатурного набора.

Отличиями предлагаемого подхода являются:

- ◆ возможность текстонезависимого анализа динамической биометрии различной модальности, произвольного объема и содержания;
- ◆ замена интегральной оценки результатов анализа биометрических данных за фиксированный период времени, применяемой в традиционных подходах к непрерывной оценке биометрических данных в темпе их поступления, с возможностью своевременного принятия решения о присутствии «чужого»;
- ◆ применение иммунологической МКС, которая хорошо согласуется с большинством задач динамической идентификации личности, использующих режим верификации, что позволяет существенно уменьшить число детекторов, необходимых для эффективного распознавания биометрических данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Ахмад Х.М., Жирков В.Ф.* Введение в цифровую обработку речевых сигналов. – Владимир: Изд-во Владим. гос. ун-та, 2007. – 192 с.
2. *Матвеев Ю.Н.* Технологии биометрической идентификации личности по голосу и другим модальностям // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение». – 2012. – № 2. – С. 46-61.
3. *Campbell W., Assaleh K., Broun C.* Speaker recognition with polynomial classifiers // IEEE Trans. Speech Audio Process. – 2002. – Vol. 10, No. 4. – P. 205-212.
4. *Анисимова Э.С.* Идентификация онлайн-подписи с помощью оконного преобразования Фурье и радиального базиса // Компьютерные исследования и моделирование. – 2014. – Т. 6, № 3. – С. 357-364.
5. *Jain A.K., Friederike D.G., Connel S.D.* On-line signature verification // Pattern Recognition. – 2002. – Vol. 35 (12). – P. 2963-2972.
6. *Plamondon R., Srihari S.* On-line and Off-line Handwriting Recognition: A Comprehensive Survey // IEEE Trans. PAMI. – 2000. – Vol. 22 (1). – P. 63-84.
7. *Иванов А.И.* Биометрическая идентификация личности по динамике подсознательных движений: монография. – Пенза: Изд-во Пенз. гос. ун-та, 2000. – 188 с.
8. *Брюхомицкий Ю.А., Казарин М.Н.* Система аутентификации личности по почерку // Сб. трудов научно-практической конференции с международным участием «Информационная безопасность». – Таганрог: Изд-во ТРТУ, 2002. – С. 22-29.
9. *Мазниченко Н.И., Гвозденко М.В.* Анализ возможностей систем автоматической идентификации клавиатурного почерка // Вестник Национального технического университета «Харьковский политехнический институт». Серия «Информатика и моделирование». – 2008. – Вып. № 24. – С. 77-82.
10. *Скубицкий А.В.* Анализ применимости метода реконструкции динамических систем в системах биометрической идентификации по клавиатурному почерку // Инфокоммуникационные технологии. – 2008. – Т. 6, № 1. – С. 51-53.
11. *Брюхомицкий Ю.А., Казарин М.Н.* Метод биометрической идентификации пользователя по клавиатурному почерку на основе разложения Хаара и меры близости Хэмминга // Известия ТРТУ. – 2003. – № 4 (33). – С. 141-149.
12. *Брюхомицкий Ю.А.* Цепочный метод клавиатурного мониторинга // Известия ЮФУ. Технические науки. – 2009. – № 11 (100). – С. 135-145.
13. *Dasgupta D.* Artificial Immune Systems and Their Applications, Ed., Springer-Verlag, 1999.
14. *De Castro L.N., Timmis, J.I.* Artificial Immune Systems: A New Computational Intelligence Approach, London: Springer-Verlag, 2000. – 357 p.
15. *Hofmeyr S. and Forrest S.* Architecture for an Artificial Immune System // Evolutionary Computation. – 2000. – No. 8 (4). – P. 443-473.
16. *Forrest S., Perelson A.S., Allen L., Cherukuri R.* Self-nonsel self discrimination in a computer // Research in Security and Privacy: Proceedings of IEEE Computer Society Symposium. – Los Alamitos: IEEE Computer Society Press, 1994. – P. 202-212.
17. *Ji Z., Dasgupta D.* Real-valued negative selection algorithm with variable-sized Detectors // Proceedings of the Genetic and Evolutionary Computation, Seattle. – 2004, Springer. – Verlag: Seattle, WA, USA, 2004. – P. 287-298.
18. *Ji Z., Dasgupta D.* Revisiting negative selection algorithm // Evolutionary Computation. – 2007. – Vol. 15. – № 2 (Summer). – P. 223-251.

19. De Castro L.N., Von Zuben F.J. The Clonal Selection Algorithm with Engineering Applications, submitted to GECCO'00. – 2000. – P. 36-37.
20. De Castro L.N., Von Zuben F.J. Learning and optimization using the clonal selection principle // IEEE Transactions on Evolutionary Computation, Special Issue on Artificial Immune Systems. – 2002. – Vol. 6. – No. 3. – P. 239-251.
21. Брюхомицкий Ю.А., Казарин М.Н. Методы многосвязного представления клавиатурного почерка // Материалы III Международной конференции «Нелокальные краевые задачи и родственные проблемы математической биологии, информатики и физики. – Нальчик, 5-8 декабря 2006 г. – С. 68-69.
22. Брюхомицкий Ю.А. Иммунологический метод верификации рукописи с использованием векторного представления данных // Известия ЮФУ. Технические науки. – 2016. – № 9 (182). – С. 50-57.
23. Брюхомицкий Ю.А. Клавиатурный мониторинг на основе иммунологического клонирования // Безопасность информационных технологий. – 2016. – № 4 (40). – С. 5-11.

REFERENCES

1. Akhmad Kh.M., Zhirkov V.F. Vvedenie v tsifrovuyu obrabotku rechevykh signalov [introduction to digital speech signal processing]. Vladimir: Izd-vo Vladim. gos. un-ta, 2007, 192 p.
2. Matveev Yu.N. Tekhnologii biometricheskoy identifikatsii lichnosti po golosu i drugim modal'nostyam [Technologies of biometric identification by voice and other modalities], *Vestnik MGTU im. N.E. Baumana. Seriya «Priborostroenie»* [Herald of the Bauman Moscow State Technical University. Series Instrument Engineering], 2012, No. 2, pp. 46-61.
3. Campbell W., Assaleh K., Broun C. Speaker recognition with polynomial classifiers, *IEEE Trans. Speech Audio Process.*, 2002, Vol. 10, No. 4, pp. 205-212.
4. Anisimova E.S. Identifikatsiya onlayn-podpisi s pomoshch'yu okonnogo preobrazovaniya Fur'e i radial'nogo bazisa [Identification of an online signature using a window Fourier transform and a radial basis], *Komp'yuternye issledovaniya i modelirovanie* [Computer studies and modeling], 2014, Vol. 6, No. 3, pp. 357-364.
5. Jain A.K., Friederike D.G., Connel S.D. On-line signature verification, *Pattern Recognition*, 2002, Vol. 35 (12), pp. 2963-2972.
6. Plamondon R., Srihari S. On-line and Off-line Handwriting Recognition: A Comprehensive Survey, *IEEE Trans. PAMI*, 2000, Vol. 22 (1), pp. 63-84.
7. Ivanov A.I. Biometricheskaya identifikatsiya lichnosti po dinamike podsoznatel'nykh dvizheniy: monografiya [Biometric identification of personality by the dynamics of subconscious movements: monograph]. Penza: Izd-vo Penz. gos. un-ta, 2000, 188 p.
8. Bryukhomitskiy Yu.A., Kazarin M.N. Sistema autentifikatsii lichnosti po pocherku [Handwriting authentication system], *Sb. trudov nauchno-prakticheskoy konferentsii s mezhdunarodnym uchastiem «Informatsionnaya bezopasnost'»* [Proceedings of scientific-practical conference with international participation "Information security"]. Taganrog: Izd-vo TRTU, 2002, pp. 22-29.
9. Maznichenko N.I. Gvozdenko M.V. Analiz vozmozhnostey sistem avtomaticheskoy identifikatsii klaviaturnogo pocherka [Analysis of the possibilities of automatic identification systems of keyboard handwriting], *Vestnik Natsional'nogo tekhnicheskogo universiteta «Khar'kovskiy politekhnicheskii institut». Seriya «Informatika i modelirovanie»* [Bulletin of the national technical University "Kharkiv Polytechnic Institute". Series "Informatics and modeling"], 2008, Issue No. 24, pp. 77-82.
10. Skubitskiy A.V. Analiz primenimosti metoda rekonstruktsii dinamicheskikh sistem v sistemakh biometricheskoy identifikatsii po klaviaturnomu pocherku [Analysis of the applicability of the method of reconstruction of dynamic systems in systems of biometric identification by keyboard handwriting], *Infokommunikatsionnye tekhnologii* [Information and communication technology], 2008, Vol. 6, No. 1, pp. 51-53.
11. Skubitskiy A.V. Analiz primenimosti metoda rekonstruktsii dinamicheskikh sistem v sistemakh biometricheskoy identifikatsii po klaviaturnomu pocherku [The method of biometric identification of the user at the keyboard handwriting based on the decomposition of the Haar and proximity measure of the Hamming], *Infokommunikatsionnye tekhnologii* [Izvestiya TSURE], 2008, Vol. 6, No. 1, pp. 51-53.

12. Bryukhomitskiy Yu.A. Tsepochnyy metod klaviaturnogo monitoringa [Chained method keyboard monitoring], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2009, No. 11 (100), pp. 135-145.
13. Dasgupta D. Artificial Immune Systems and Their Applications, Ed., Springer-Verlag, 1999.
14. De Castro L.N., Timmis, J.I. Artificial Immune Systems: A New Computational Intelligence Approach, London: Springer-Verlag, 2000, 357 p.
15. Hofmeyr S. and Forrest S. Architecture for an Artificial Immune System, *Evolutionary Computation*, 2000, No. 8 (4), pp. 443-473.
16. Forrest S., Perelson A.S., Allen L., Cherukuri R. Self-nonsel self discrimination in a computer, *Research in Security and Privacy: Proceedings of IEEE Computer Society Symposium*. Los Alamitos: IEEE Computer Society Press, 1994, pp. 202-212.
17. Ji Z., Dasgupta D. Real-valued negative selection algorithm with variable-sized Detectors, *Proceedings of the Genetic and Evolutionary Computation, Seattle. 2004*, Springer. Verlag: Seattle, WA, USA, 2004, pp. 287-298.
18. Ji Z., Dasgupta D. Revisiting negative selection algorithm, *Evolutionary Computation*, 2007, Vol. 15, No. 2 (Summer), pp. 223-251.
19. De Castro L.N., Von Zuben F.J. The Clonal Selection Algorithm with Engineering Applications, submitted to GECCO'00, 2000, pp. 36-37.
20. De Castro L.N., Von Zuben F.J. Learning and optimization using the clonal selection principle, *IEEE Transactions on Evolutionary Computation, Special Issue on Artificial Immune Systems*, 2002, Vol. 6, No. 3, pp. 239-251.
21. Bryukhomitskiy Yu.A., Kazarin M.N. Metody mnogosvyaznogo predstavleniya klaviaturnogo pocherka [Methods of multi-linked representation of keyboard handwriting], *Materialy III Mezhdunarodnoy konferentsii «Nelokal'nye kraevye zadachi i rodstvennye problemy matematicheskoy biologii, informatiki i fiziki* [Materials of the III International conference " Nonlocal boundary value problems and related problems of mathematical biology, Informatics and physics]. Nal'chik, 5-8 dekabrya 2006, pp. 68-69.
22. Bryukhomitskiy Yu.A. Immunologicheskiiy metod verifikatsii rukopisi s ispol'zovaniem vektornogo predstavleniya dannykh [Immunological method of manuscript verification using vector data representation], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2016, No. 9 (182), pp. 50-57.
23. Bryukhomitskiy Yu.A. Klaviaturnyy monitoring na osnove immunologicheskogo klonirovaniya [Keyboard monitoring based on immunological cloning], *Bezopasnost' informatsionnykh tekhnologiy* [Information technology security], 2016, No. 4 (40), pp. 5-11.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Брюхомицкий Юрий Анатольевич – Южный федеральный университет; e-mail: bryuhomitskiy@sfedu.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; с.н.с.; доцент.

Bryuhomitsky Yuriy Anatoly – Southern Federal University; e-mail: bryuhomitskiy@sfedu.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; senior researcher; associate professor.