Чудин Кирилл Сергеевич – e-mail: 4ydo-kirill@rambler.ru; тел.: +79653295515; кафедра защиты информации; ассистент.

Болычев Максим Владимирович – e-mail: Nat15171@yandex.ru; тел.: +79167260955; кафедра защиты информации; соискатель.

Kondakov Sergey Evgenievch – Bauman Moscow State Technical University; e-mail: sergeikondakov@list.ru; Moscow, Russia; phone: +79037947857; the department of information security; can. of eng. sc.

Chudin Kirill Sergeevich – e-mail: 4ydo-kirill@rambler.ru; phone: +79653295515; the department of information security; assistant.

Bolychev Maxim Vladimirovich – e-mail: Nat15171@yandex.ru; phone: +79167260955; the department of information security; applicant.

УДК 004.067 DOI 10.18522/2311-3103-2023-2-80-89

Ю.А. Брюхомицкий

ИММУНОЛОГИЧЕСКАЯ МОДЕЛЬ КЛАВИАТУРНОГО МОНИТОРИНГА ОПЕРАТОРОВ ИНФОРМАЦИОННЫХ СИСТЕМ

Целью работы является разработка модели клавиатурного мониторинга операторов информационных систем, основанной на использовании цепочного метода учета параметров клавиатурного почерка. Указанный метод предусматривает оценку клавиатурного почерка оператора на цепочках символов заданной длины, отражающих лингвистически связанные параметры клавиатурного набора, характерные для данного оператора. Клавиатурный набор таких цепочек оператором с «хорошим» клавиатурным почерком обладает существенно более высокой индивидуальностью, обусловленной корреляционными зависимостями между временными параметрами последовательно идущих символов и пауз. В итоге цепочный метод позволяет обеспечить более высокую точность верификации личности оператора. Клавиатурный мониторинг на основе цепочного метода предлагается реализовать в базисе искусственных иммунных систем с использованием иммунологической модели клональной селекции, в которой детекторы представлены идентификационными параметрами области распределения клавиатурных параметров «своего». В задачах клавиатурного мониторинга область распределения клавиатурных параметров верифицируемого оператора всегда существенно меньше совокупной области распределения клавиатурных параметров других возможных операторов. Выбор указанной модели позволяет существенно снизить необходимый объем популяции детекторов, и как следствие, – существенно сократить время верификации работающего оператора. Принятие решения о подмене «своего» оператора «чужим» предлагается считать обоснованным при превышении частоты срабатывания детекторов установленного порогового значения. Предложенная иммунологическая модель обладает рядом преимуществ. Использование цепочного метода учета клавиатурных параметров позволяет с бóльшей точностью верифицировать оператора, в сравнении с традиционными методами. Используемая модель клональной селекции в сочетании с векторным представлением клавиатурных данных позволяет существенно ускорить процесс обучения и сократить время, необходимое для своевременного принятия решения о присутствии «чужого» оператора. Важным достоинством модели является возможность обучаться исключительно на примерах клавиатурного почерка оперативно доступных «своих» операторов. Использование модели клональной селекции позволяет также существенно снизить необходимый объем популяции детекторов, способных эффективно «покрыть» область распределения клавиатурных параметров «своего» оператора.

Цепочный метод клавиатурного мониторинга операторов информационных систем; иммунологическая модель клональной селекции с положительным отбором; верификация работающего оператора по принципу «свой-чужой».

Yu.A. Bryuhomitsky

IMMUNOLOGICAL MODEL OF KEYBOARD MONITORING OF INFORMATION SYSTEM OPERATORS

The purpose of this work is to develop a model of keyboard monitoring of information system operators, based on the use of a chain method of accounting keyboard handwriting parameters. The specified method provides estimation of operator's keyboard handwriting on chains of characters of given length, reflecting linguistically related parameters of keyboard set, characteristic for the given operator. The keyboard typing of such chains by the operator with "good" keyboard handwriting has significantly higher individuality due to correlation dependences between the time parameters of successive characters and pauses. As a result, the chain method allows to provide higher accuracy of operator's identity verification. Keyboard monitoring based on the chain method is proposed to be implemented in the basis of artificial immune systems using an immunological model of clonal selection, in which the detectors are represented by identifying parameters of the distribution area of the keyboard parameters of "friend". In the tasks of keyboard monitoring the area of distribution of keyboard parameters of the verified operator is always significantly less than the cumulative area of distribution of keyboard parameters of other possible operators. The choice of the specified model allows to significantly reduce the required volume of the detector population, and as a consequence - to significantly reduce the verification time of the working operator. The decision to replace "friend" operator with "stranger" is proposed to be considered reasonable when the frequency of operation of detectors exceeds the established threshold value. The proposed immunological model has a number of advantages. The use of the chain method of keyboard parameters accounting allows to verify the operator with greater accuracy in comparison with traditional methods. The clonal selection model in combination with vector representation of the keyboard data allows to significantly speed up the learning process and reduce the time required to make a timely decision on the presence of a "stranger" operator. An important advantage of the model is the ability to learn solely from the examples of keyboard handwriting operationally available "friend" operators. The use of the clonal selection model also makes it possible to significantly reduce the required volume of the population of detectors capable of effectively "covering" the distribution area of the keyboard parameters of "friend" operator.

Chain method of keyboard monitoring of information system operators; immunological model of clonal selection with positive selection; verification of working operator by the principle of "friend-or-stranger".

Введение. Для обеспечения безопасности информационных систем (ИС) в ракурсе возможных нарушений и злоупотреблений со стороны операторов этих систем могут эффективно применяться современные биометрические технологии клавиатурного мониторинга [1, 2]. Клавиатурный мониторинг позволяет верифицировать личность оператора путем непрерывного текстонезависимого анализа его клавиатурного почерка. При необходимости клавиатурный мониторинг может проводиться скрытно (прозрачно) для операторов. Система клавиатурного мониторинга (СКМ) позволяют решать ряд важных задач для обеспечения информационной безопасности ИС, которые трудно решаются другими методами:

- непрерывная (при необходимости скрытная) верификация личности оператора в процессе его клавиатурной работы в ИС;
- скрытное выявление операторов-инсайдеров, совершающих неправомерные и злонамеренные действия, ставящие под угрозу информационную безопасность ИС;
- скрытное выявление отклонений психофизических характеристик операторов ИС критических приложений, характеризующихся высокой ценой ошибки оператора;
- тестирование (при необходимости скрытное) кандидатов на должность операторов ИС критических приложений, характеризующихся высокой ценой ошибки оператора;
- контролировать правдивость ответов операторов на заданные вопросы в процессе аудита нарушений безопасности ИС (аналог «детектора лжи»).

При реализации СКМ первостепенное значение имеют параметры точности и скорости верификации личности работающего оператора, которые, определяются способами представления и классификации клавиатурных биометрических параметров, а также – подходами и методами, используемыми для реализации процедуры верификации.

Известные методы построения СКМ основаны на прямом измерении параметров клавиатурной работы оператора: длительностей удержания и пауз между удержаниями одиночных клавиш [3–7]. Недостатком метода является низкая точность верификации личности оператора, обусловленная, недостаточной информативностью представления его индивидуальных клавиатурных параметров.

Постановка задачи. Автором статьи был предложен цепочный метод построения СКМ, отличающийся от известных тем, что временные параметры клавиатурного набора измеряются на последовательно идущих цепочках заданной длины, содержащих лингвистически связанные совокупности символов и пауз [8–10]. Клавиатурный набор таких цепочек оператором с «хорошим» клавиатурным почерком обладает существенно более высокой индивидуальностью, обусловленной корреляционными зависимостями между временными параметрами последовательно идущих символов и пауз. В итоге цепочный метод обладает более высокой точностью верификации личности оператора, но при этом требует существенно бóльших вычислительных затрат.

При использовании цепочного метода множество всех событий клавиатуры в терминах формальных грамматик рассматривается как алфавит A, состоящий из двух подмножеств $\mathrm{A} = \mathrm{A_y} \cup \mathrm{A_п}$:

$\mathrm{A_y} \subset \mathrm{A}$ – события клавиатуры, состоящие в удержании одной из n клавиш;

$\mathrm{A_п} \subset \mathrm{A}$ – события клавиатуры, состоящие в наличии пауз между удержаниями очередных клавиш или перекрытий времен удержаний смежных при наборе клавиш.

Ограниченные последовательности событий клавиатуры множества A, ориентированные слева направо, начинающиеся и оканчивающиеся событиями из подмножества $\mathrm{A_y}$, трактуются как цепочки событий $T_{i_1,i_2,\dots,i_p}$. Длиной r цепочки является общее число событий алфавита A, входящих в цепочку: $\left|T_{i_1,i_2,\dots,i_p}\right| = r$, $i_1, i_2, \dots, i_p = 1, 2, \dots, n$. При клавиатурном наборе события из множеств $\mathrm{A_y}$ и $\mathrm{A_п}$ строго чередуются, поэтому в каждой цепочке длины r будет содержаться p событий множества $\mathrm{A_y}$ и $q = p - 1$ событий множества $\mathrm{A_п}$. Длина цепочки всегда есть целое нечетное число $r = p + q = 2p - 1 = 1, 3, 5, \dots$. Для заданного числа контролируемых клавиш n и заданной длины цепочек r суть цепочного метода в терминах формальных грамматик состоит в формировании всех возможных цепочек событий алфавита A длины r в пространстве размерности $p = (r + 1)/2 = q + 1$.

Для представления клавиатурных параметров цепочным методом в поле действительных чисел P задается пространственная матрица размерности p

$$\mathrm{T}^p = \left\| T_{i_1,i_2,\dots i_p} \right\|, \quad i_1, i_2, \dots, i_p = 1, 2, \dots, n, \quad p = 2, 3, \dots,$$

состоящая, в общем случае, из n^p элементов, представленных цепочками $T_{i_1,i_2,\dots i_p,}$ $i_1, i_2, \dots, i_p = 1, 2, \dots, n,$ $p = 2, 3, \dots$. При этом каждая цепочка длины r будет содержать r временных параметров из числового поля P. Для реальных алфавитов A, содержащих ограниченное число учитываемых при клавиатурном наборе символов, а также не используемых сочетаний из более двух одинаковых последовательно идущих символов, общее число элементов матрицы T^p будет всегда меньшим, чем n^p.

Для описания и последующего использования пространственной матрицы T^p, она представляется совокупностью своих сечений с фиксированным значением одного i_α или двух индексов i_α, i_β. В первом случае образуется совокупность про-

стых сечений ориентации i_α, являющихся $(p-1)$-мерными матрицами n-го порядка. Во втором случае образуется совокупность двукратных сечений ориентации i_α, i_β, являющихся $(p-2)$-мерными матрицами n-го порядка.

При реализации цепочного метода длина цепочки $r = \left|T_{i_1,i_2,\ldots,i_p}\right|$ выбирается фиксированной по формуле $r = 3 + 2l$, где $l = 0, 1, 2, \ldots$.

Цепочный метод фактически использует многомерное представление клавиатурных параметров, при котором каждой цепочке соответствует точка (ξ_1, ξ_2, …, ξ_p) в пространстве мерности p с координатами ξ_k, k = 1, 2, …, p, определяемыми событиями $i_p = 1, 2, \ldots, n$ подмножества $\mathbf{A}_y$. На рис. 1 – пример представления цепочным методом слова «почерк» с длиной цепочек r = 5 в пространстве мерности p = 3.

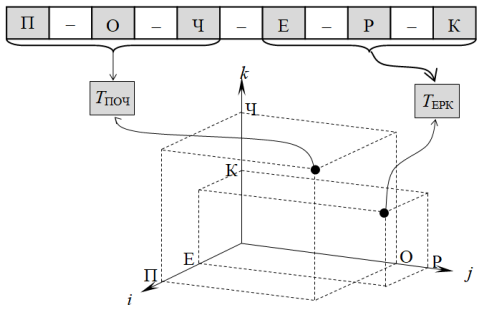

Рис. 1. Пример представления цепочным методом клавиатурного набора слова «почерк» с заданной длиной цепочек r = 5 в пространстве мерности p = 3

В цепочном методе идентифицирующие личность оператора клавиатурные параметры определяются цепочками лингвистически связанных событий, характеризующихся выраженной индивидуальностью их воспроизведения данным оператором. Такое представление параметров клавиатурного набора хорошо согласуется с принципами представления и анализа информационных потоков, принятыми в искусственных иммунных системах (ИИС) [11–25].

Решение поставленной задачи. Построение СКМ на основе цепочного метода в базисе ИИС предлагается реализовать с использованием иммунологической модели, реализующей децентрализованную верификацию личности оператора, основанную на сопоставлении последовательности информационных единиц, представленными цепочками его клавиатурных параметров, с предварительно созданными детекторами. В ИИС применяется две основных модели сопоставления последовательности информационных единиц с детекторами. «Модель отрицательного отбора (МОО)», в которой детекторы представлены идентификационными параметрами совокупной области распределения «чужих» и «модель клональной селекции (МКС)», в которой детекторы представлены идентификационными параметрами области распределения «свой». Выбор модели предопределяет необходимый объем популяции детекторов, способных эффективно «покрыть» соответствующую область распределения параметров. В СКМ область распределения клавиатурных параметров верифицируемого оператора («свой») как правило существенно меньше совокупной области распределения клавиатурных параметров других возможных операторов («область чужие»). Это обстоятельство определяет целесообразность применения в СКМ иммунологической модели МКС.

Другой разновидностью применяемых иммунологических моделей является используемый способ представления информационных единиц данных: строковый или векторный. Исходя из описания цепочного метода СКМ, следует, что адекватным представлением для реализации этого метода является векторное представление данных.

МКС содержит две фазы: обучения и верификации.

В фазе обучения в МКС осуществляется генерация начальной популяции детекторов в метрике клавиатурных параметров цепочного метода СКМ с последующим отбором тех из них, которые в пространстве признаков в наибольшей степени соответствуют личности оператора «свой». Входящие в начальную популяцию детекторы подвергаются затем операциям клонирования и гипермутации, что позволяет существенно увеличить популяцию детекторов области «свой». Итогом фазы обучения является рабочая популяция детекторов области «свой», которая размещается в памяти МКС.

В фазе верификации клавиатурные параметры работающего оператора ИС сопоставляются с рабочей популяцией детекторов «свой». При сопоставлении проверяется априори установленный «уровень близости» для сравниваемых параметров. Принятие конечного решения о том, кому принадлежит анализируемый клавиатурный почерк «своему» или «чужому», осуществляется на основе статистического подхода, при котором контролируется частота выполнения условия близости.

Реализация модели осуществляется в r-мерном Евклидовом пространстве E^r, ограниченном рабочим подпространством $E_p^r \subset E^r$, определяемом минимаксными значениями координат $x_1, x_2, \dots, x_r$ векторов признаков $x_i = x_1, x_2, \dots, x_r$, соответствующих предельным значениям временных параметров τ_i и $\tau_{i,j}$, $i, j = 1, 2, \dots, n$ событий клавиатуры для верифицируемого оператора. Точки пространства E^r, представленные векторами признаков $x_i = x_{1i}, x_{2i}, \dots, x_{ni}$, можно трактовать как последовательность $\mathrm{X}_i = x_1, x_2, \dots$, которая «пробегает» конечное множество Ψ_x векторов клавиатурных признаков x_i верифицируемого оператора. Далее последовательность X_i расчленяется на фрагменты по r отсчетов x_i в каждом фрагменте. Результатом будет новая последовательность $\mathrm{Y}_j = y_1, y_2, \dots$, $j = 1, 2, \dots$, каждый элемент y_j которой содержит r n-мерных векторов x_i исходной последовательности X_i:

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

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:

$$y_j = \begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1r} \\ y_{21} & y_{22} & \cdots & y_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ y_{n1} & y_{n2} & \cdots & y_{nr} \end{bmatrix}.$$

В итоге образ клавиатурной биометрии оператора будет представлен последовательностью Y_j s-мерных векторов признаков y_j в пространстве признаков E^s.

Последовательность Y_j, ограниченная N_y элементами $\overline{\mathrm{Y}}_j = y_1, y_2, \dots, y_{N_y}$, $j = 1, 2, \dots N_y$, можно трактовать как клавиатурный эталон оператора.

В фазе обучения ИИС вначале создается начальная популяция детекторов в метрике векторов y_j. Затем по принципу положительного отбора выявляются детекторы из начальной популяции, которые в пространстве E^s наиболее близки между собой. При этом степень близости векторов моделирует свойство аффинности клеток иммунной системы. Детекторы, отобранные из начальной популяции, на основе итерационной процедуры подвергаются клонированию, гипермутации и последующему отбору. Останов процедуры обучения осуществляется по определенным признакам, свидетельствующим о достижении достаточной степени покрытия популяцией детекторов области распределения клавиатурных параметров данного оператора.

На этапе распознавания клавиатурные параметры Y_j верифицируемой личности сравниваются с детекторами популяции «своего» по принципу близости. Соотношение числа сработавших детекторов к их общему числу позволяет сделать оценку вероятности для принятия системой решения «свой–чужой».

1. Создание в пространстве E^r путем случайной генерации (с равномерным законом распределения) начальной популяции детекторов $\mathrm{D}_k^{\lambda} = d_1, d_1, \ldots, d_{N_d}$, $\lambda = 0,\ k = 1, 2, \ldots, N_d$ представленных векторами в формате векторов y_j.

2. Для каждой пары $d_k \in \mathrm{D}_k^{\lambda}$ и $y_j \in \overline{\mathrm{Y}}_j$ вычисляется степень их взаимной аффинности. В качестве меры аффинности a_{kj} используется Евклидово расстояние между векторами d_k и y_j:

$$a_{kj}(d_k, y_j) = \sqrt{\sum_{p=1}^{N} \left(d_{kp} - y_{jp}\right)^2}, \quad p = 1, 2, \ldots, N, \quad N = N_d \cdot N_y.$$

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

$$\mathrm{A}\left\|a_{kj}(d_k, y_j)\right\| = \left\| \begin{matrix} a_{11} & a_{12} & \ldots & a_{1N_y} \\ a_{21} & a_{22} & \ldots & a_{2N_y} \\ \ldots & \ldots & \ldots & \ldots \\ a_{N_d 1} & a_{N_d 2} & \ldots & a_{N_d N_y} \end{matrix} \right\|, k = 1, 2, \ldots, N_d, j = 1, 2, \ldots, N_y.$$

3. Из каждого столбца матрицы A отбирается l из N_d детекторов d_k, соответствующих наибольшей взаимной аффинности $a_{kj}(d_k, y_j)$, $k = 1, 2, \ldots, l$, $j = 1, 2, \ldots, N_y$ и подвергаются операции клонирования C:

$$C[d_k] = d_k^c, \qquad k = 1, 2, \ldots, l \quad c = 1, 2, \ldots, q$$

Количество образуемых клонов q_k каждого из l детекторов d_k^c пропорционально взаимной аффинности $a_{kj}(d_k, y_j)$: $q_k \propto k_c \cdot a_{kj}(d_k, y_j)$, где – k_c коэффициент пропорциональности при клонировании. При этом общее количество образованных клонов должно оставаться равным N_d:

$$\sum_{k=1}^{l} q_k = \left\lfloor \sum_{k=1}^{l} k_c \cdot a_{kj}(d_k, y_j) \right\rfloor = N_d.$$

Таким образом все детекторы популяции D_k^{λ} заменяются клонами d_k^c: $\mathrm{D}_k^{\lambda} \to \mathrm{D}_k^{\lambda c}$. Очевидно, что для выполнения этого условия

$$k_c = {N_d}\Big/{\sum_{k=1}^{l} a_{kj}(d_k, y_j)}.$$

Операция клонирования повышает вероятность покрытия детекторами областей распределения клавиатурных параметров y_j.

4. Все клоны d_k^c популяции $\mathrm{D}_k^{\lambda c}$ подвергаются операции гипермутации G:

$$G[d_k^c] = d_k^{cG}, \qquad k = 1, 2, \ldots, l \quad c = 1, 2, \ldots, q.$$

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

$$G \propto k_m \,/\, a_{kj}(d_k, y_j),$$

где – k_m – коэффициент гипермутации клонов d_k^{cG} определяемый из условия: $m = 1$ при $\max_{k=1,2,\ldots,l} a_{kj}(d_k, y_j)$

Операция гипермутации сужает область поиска новых эффективных детекторов.

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

5. Для каждой пары $d_k^{cG} \in \mathrm{D}_k^{\lambda cG}$ и $y_j \in \overline{\mathrm{Y}}_j$ вычисляется степень взаимной аффинности.

$$a_{kj}\left(d_k^{cG}, y_j\right) = \sqrt{\sum_{p=1}^{N}\left(d_{kp}^{cG} - y_{jp}\right)^2}, \qquad p = 1, 2, \dots, N.$$

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

$$\mathrm{A}\left\|a_{kj}\left(d_k^{cG}, y_j\right)\right\|, \; k = 1, 2, \dots, N_d \qquad j = 1, 2, \dots, N_y.$$

6. Из каждого столбца матрицы A отбирается совокупность из l детекторов d_k^{cG}, соответствующих наибольшей взаимной аффинности $a_{kj}\left(d_k^{cG}, y_j\right)$, $k = 1, 2, \dots, l, \; j = 1, 2, \dots, N_y$. Полученные детекторы d_k^{cGm} образуют популяцию детекторов памяти D^{M}.

7. Проверка условия останова: при выполнении условия, – переход на шаг 9, иначе следующий шаг.

8. $(N_d - l)$ детекторов популяции $\mathrm{D}_k^{\lambda cG}$, обладающих наименьшей аффинностью $a_{kj}\left(d_k, y_j\right)$ заменяются новыми, путем случайной генерации (с равномерным законом распределения) новой популяции детекторов $\mathrm{D}_k^{\lambda} = d_1, d_1, \dots, d_{N_d}, \quad \lambda = \lambda + 1,$ $k = 1, 2, \dots, (N_d - l)$ представленных векторами в формате векторов y_j.

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

В фазе распознавания элементы y_j анализируемой последовательности клавиатурных параметров Y_j сопоставляются с детекторами d_k^M популяции памяти D^M, $k = 1, 2, \dots, N_M$ с использованием меры близости Евклида между векторами y_j и d_k^M:

$$\nabla\left(y_j, d_k^M\right) = \sqrt{\sum_{\upsilon=1}^{s}\left(y_{j\upsilon} - d_{k\upsilon}\right)^2}.$$

Критический уровень близости $\nabla\left(y_j, d_k^M\right) = \nabla^*$ определяет границу для принятия СКМ решения «свой/чужой» и задается, исходя из допустимых ошибок первого рода. Если для некоторой пары y_j и d_k^M $\nabla\left(y_j, d_k^M\right) > \nabla^*$, то считается, что элемент y_j анализируемой биометрии Y_j, принадлежит «чужому».

Существенные вариации клавиатурных параметров в последовательностях Y_j и значительные размеры самих последовательностей Y_j определяют целесообразность применения статистического подхода для принятия СКМ решения «свой»-«чужой» [22, 23]. При таком подходе контролируется частота f выполнения условия $\nabla\left(y_j, d_k^M\right) > \nabla^*$, которая определяет статистическую вероятность принадлежности клавиатурных параметров «чужому»:

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

где n_{∇}^{+} число случаев выполнения условия $\nabla\left(y_j, d_k^M\right) > \nabla^*$ в n_{∇} проведенных операциях сопоставлений y_j с d_k^M.

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

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

где $\mathrm{Y}_j^{\text{с}}$– последовательность биометрических признаков «своего»; $\mathrm{Y}_j^{\text{ч}}$– последовательность векторов признаков «чужого»;

Заключение. Предложенная иммунологическая модель клавиатурного мониторинга операторов ИС потенциально обладает рядом преимуществ.

Временные параметры клавиатурного набора текста оператором с «хорошим» клавиатурным почерком обладает существенно более высокой индивидуальностью, обусловленной корреляционными зависимостями между временными параметрами последовательно идущих символов и пауз. Это позволяет с бóльшей точностью верифицировать оператора ИС, чем традиционные методы КМ на основе прямых измерений клавиатурных параметров.

Используемая в СКМ модель клональной селекции обладает высокой скоростью сходимости при решении задач классификации. В сочетании с принятым векторным представлением клавиатурных данных она позволяет существенно ускорить процесс обучения СКМ, а также сократить время, необходимое для своевременного принятия решения о наличии в ИС «чужого» оператора.

Важным достоинством применяемой в СКМ модели клональной селекции является возможность обучаться исключительно на примерах клавиатурного почерка «своих» операторов ИС, которые всегда оперативно доступны для обучения в СКМ.

Выбор модели клональной селекции для СКМ позволяет также существенно снизить необходимый объем популяции детекторов, способных эффективно «покрыть» априори доступную область распределения клавиатурных параметров «своего» оператора.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Брюхомицкий Ю.А.* Клавиатурная идентификация личности. – Lambert Academic Publishing, Saarbrűcken, Germany, 2012. – 140 с. – ISBN 978-3-8484-1119-1.
2. *Файсханов И.Ф.* Аутентификация пользователей при помощи устойчивого клавиатурного почерка со свободной выборкой текста // Кибернетика и программирование. – 2018. № 3. – С. 72-86.
3. *Yevetskiy V., Horniichuk I.* Use of keyboard handwriting in user authentication systems // Information Technology and Security. – 2016. – Vol. 4, Issue 1. – P. 27-33.
4. *Вязигин А.А., Тупикина Н.Ю., Сыпин Е.В.* Разработка и реализация программы для биометрии пользователя персонального компьютера на базе определения параметров клавиатурного почерка // Южно-Сибирский научный вестник. – 2019. – № 1 (25). – С. 43-48.
5. *Аверин А.И., Сидоров Д.П.* Аутентификация пользователей по клавиатурному почерку // Огарев-online. – 2015. – № 20. – Режим доступа: https://journal.mrsu.ru/arts/autentifikaciya-polzovatelej-po-klaviaturnomu-pocherku.
6. *Joyce R., Gupta G.* Identity Authentication Based on Keystroke Latencies. – http://www.cs.cmu.edu/~maxion/courses/JoyceGupta90.pdf.
7. *Monrose F.* Keystroke Dynamics as a Biometric for Authentication. – http://avirubin.com/fgcs.pdf.
8. *Roth J., Liu X., Ross A.* Biometric Authentication via Keystroke Sound. – http://www.cse.msu.edu/~liuxm/publication/Roth_Liu_Ross_Metaxas_ICB2013.pdf
9. *Scott M. L. et al.* Continuous Identity Verification through Keyboard Biometrics. – https://sa.rochester.edu/jur/issues/fall2005/ordal.pdf.
10. *Брюхомицкий Ю.А.* Цепочный метод клавиатурного мониторинга // Известия ЮФУ. Технические науки. – 2009. – № 11. – С. 135-145.
11. *Брюхомицкий Ю.А.* Выделение информативных биометрических параметров в системах клавиатурного мониторинга // Матер. XI Международной научно-практической конференции «Информационная безопасность». Ч. 2. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 67-72.
12. *Брюхомицкий Ю.А., Казарин М.Н.* Многосвязное представление биометрических параметров в системах клавиатурного мониторинга // Матер. XI Международной научно-практической конференции «Информационная безопасность». Ч. 2. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 72-77.
13. *Брюхомицкий Ю.А.* Иммунологический подход к организации клавиатурного мониторинга // Известия ЮФУ. Технические науки. – 2014. – № 2 (151). – С. 33-41.
14. *Брюхомицкий Ю.А.* Клавиатурный мониторинг на основе иммунологического клонирования // Безопасность информационных технологий. – 2016. – № 4 (40). – С. 5-11.

15. *Dasgupta D.* Artificial Immune Systems and Their Applications. – Springer-Verlag, 1998.
16. *De Castro L N., Timmis J.I.* Artificial Immune Systems: A New Computational Intelligence Approach. – London: Springer-Verlag, 2000. – 357 p.
17. *Hofmeyr S., Forrest S.* Architecture for an Artificial Immune System // Evolutionary Computation. – 2000. – 8 (4). – P. 443-473.
18. *De Castro L.N., Von Zuben F.J*. The Clonal Selection Algorithm with Engineering Applications, submitted to GECCO'00. – 2000. – P. 36-37.
19. *Hofmeyr S., Forrest S.* Architecture for an Artificial Immune System // Evolutionary Computation. – 8 (4). – P. 443-473.
20. *De Castro L.N., Von Zuben F.J.* Learning and optimization using the clonal se-lection principle // IEEE Transactions on Evolutionary Computation, Special Issue on Artificial Immune Systems. – 2002. – Vol. 6, No. 3. – P. 239-251.
21. *De Castro L.N. and Timmis J.I.* Artificial immune systems as a novel soft computing paradigm // Soft Computing - A Fusion of Foundations, Methodologies and Applications. – 2003. – 7 (8). – P. 526-544.
22. *Ji Z., Dasgupta D.* Real-valued negative selection algorithm with variable-sized Detectors // Proceedings of the Genetic and Evolutionary Computation, Seattle. – Springer. Verlag: Seattle, WA, USA, 2004. – P. 287-298.
23. *Ji Z., Dasgupta D.* Revisiting negative selection algorithm // Evolutionary Computation. – 2007. – Vol. 15, No. 2 (Summer). – P. 223-251.
24. Искусственные иммунные системы и их применение / под ред. Д. Дасгупты: пер. с англ. А.А. Романюхи. – М.: Физматлит, 2006. – 344 с.
25. *Dasgupta D., Yua S., Nino F*. Recent advances in artificial immune systems: Models and applications // Applied Soft Computing. – 2011. – Vol. 11. – P. 1574-1587.
26. *Зайцев С.А., Субботин С.А.* Модели и методы автоматической классификации объектов по признакам на основе иммунокомпьютинга // Радиоэлектроника, информатика, управление. – 2010. – № 2. – С. 117-124.

REFERENCES

1. *Bryukhomitskiy Yu.A.* Klaviaturnaya identifikatsiya lichnosti [Keyboard identification of the person]. Lambert Academic Publishing, Saarbrűcken, Germany, 2012, 140 p. ISBN 978-3-8484-1119-1.
2. *Fayskhanov I.F.* Autentifikatsiya pol'zovateley pri pomoshchi ustoychivogo klaviaturnogo pocherka so svobodnoy vyborkoy teksta [Authentication of users using a stable keyboard handwriting with a free selection of text], *Kibernetika i programmirovanie* [Cybernetics and programming], 2018, No. 3, pp. 72-86.
3. *Yevetskiy V., Horniichuk I.* Use of keyboard handwriting in user authentication systems, *Information Technology and Security,* 2016, Vol. 4, Issue 1, pp. 27-33.
4. *Vyazigin A.A., Tupikina N.Yu., Sypin E.V.* Razrabotka i realizatsiya programmy dlya biometrii pol'zovatelya personal'nogo komp'yutera na baze opredeleniya parametrov klaviaturnogo pocherka [Development and implementation of a program for biometrics of a personal computer user based on determining the parameters of the keyboard handwriting], *Yuzhno-Sibirskiy nauchnyy vestnik* [South Siberian Scientific Bulletin], 2019, No. 1 (25), pp. 43-48.
5. *Averin A.I., Sidorov D.P.* Autentifikatsiya pol'zovateley po klaviaturnomu pocherku [User authentication by keyboard handwriting], *Ogarev-online* [Ogarev-online], 2015, No. 20. Available at: https://journal.mrsu.ru/arts/autentifikaciya-polzovatelej-po-klaviaturnomu-pocherku.
6. *Joyce R., Gupta G.* Identity Authentication Based on Keystroke Latencies. Available at: http://www.cs.cmu.edu/~maxion/courses/JoyceGupta90.pdf.
7. *Monrose F.* Keystroke Dynamics as a Biometric for Authentication. Available at: http://avirubin.com/fgcs.pdf.
8. *Roth J., Liu X., Ross A.* Biometric Authentication via Keystroke Sound. Available at: http://www.cse.msu.edu/~liuxm/publication/Roth_Liu_Ross_Metaxas_ICB2013.pdf
9. *Scott M. L. et al.* Continuous Identity Verification through Keyboard Biometrics. Available at: https://sa.rochester.edu/jur/issues/fall2005/ordal.pdf.

10. *Bryukhomitskiy Yu.A.* TSepochnyy metod klaviaturnogo monitoringa [Chain method of keyboard monitoring], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2009, No. 11, pp. 135-145.
11. *Bryukhomitskiy Yu.A.* Vydelenie informativnykh biometricheskikh parametrov v sistemakh klaviaturnogo monitoringa [Identification of informative biometric parameters in keyboard monitoring systems], *Mater. XI Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Informatsionnaya bezopasnost'»* [Proceedings of the XI International Scientific and Practical Conference "Information Security"]. Part 2. Taganrog: Izd-vo TTI YuFU, 2010, pp. 67-72.
12. *Bryukhomitskiy Yu.A., Kazarin M.N.* Mnogosvyaznoe predstavlenie biometricheskikh parametrov v sistemakh klaviaturnogo monitoringa [Multi-connected representation of biometric parameters in keyboard monitoring systems], *Mater. XI Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Informatsionnaya bezopasnost'»* [Proceedings of the XI International Scientific and Practical Conference "Information Security"]. Part 2. Taganrog: Izd-vo TTI YuFU, 2010, pp. 72-77.
13. *Bryukhomitskiy Yu.A.* Immunologicheskiy podkhod k organizatsii klaviaturnogo monitoringa [Immunological approach to the organization of keyboard monitoring], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 2 (151), pp. 33-41.
14. *Bryukhomitskiy Yu.A.* Klaviaturnyy monitoring na osnove immunologicheskogo klonirovaniya [Keyboard monitoring based on immunological cloning], *Bezopasnost' informatsionnykh tekhnologiy* [Security of Information Technologies], 2016, No. 4 (40), pp. 5-11.
15. *Dasgupta D.* Artificial Immune Systems and Their Applications. Springer-Verlag, 1998.
16. *De Castro L N., Timmis J.I.* Artificial Immune Systems: A New Computational Intelligence Approach. London: Springer-Verlag, 2000, 357 p.
17. *Hofmeyr S., Forrest S.* Architecture for an Artificial Immune System, *Evolutionary Computation*, 2000,– 8 (4), pp. 443-473.
18. *De Castro L.N., Von Zuben F.J.* The Clonal Selection Algorithm with Engineering Applications, submitted to GECCO'00, 2000, pp. 36-37.
19. *Hofmeyr S., Forrest S.* Architecture for an Artificial Immune System, *Evolutionary Computation*, 8 (4), pp. 443-473.
20. *De Castro L.N., Von Zuben F.J.* Learning and optimization using the clonal se-lection principle, *IEEE Transactions on Evolutionary Computation, Special Issue on Artificial Immune Systems*, 2002, Vol. 6, No. 3, pp. 239-251.
21. *De Castro L.N. and Timmis J.I.* Artificial immune systems as a novel soft computing paradigm, *Soft Computing - A Fusion of Foundations, Methodologies and Applications*, 2003, 7 (8), pp. 526-544.
22. *Ji Z., Dasgupta D.* Real-valued negative selection algorithm with variable-sized Detectors, *Proceedings of the Genetic and Evolutionary Computation, Seattle*. Springer. Verlag: Seattle, WA, USA, 2004, pp. 287-298.
23. *Ji Z., Dasgupta D.* Revisiting negative selection algorithm, *Evolutionary Computation*, 2007, Vol. 15, No. 2 (Summer), pp. 223-251.
24. Iskusstvennye immunnye sistemy i ikh primenenie [Artificial immune systems and their application], ed. by D. Dasgupty: trans. from Engl. A.A. Romanyukhi. Moscow: Fizmatlit, 2006, 344 p.
25. *Dasgupta D., Yua S., Nino F*. Recent advances in artificial immune systems: Models and applications, *Applied Soft Computing*, 2011, Vol. 11, pp. 1574-1587.
26. *Zaytsev S.A., Subbotin S.A.* Modeli i metody avtomaticheskoy klassifikatsii ob"ektov po priznakam na osnove immunokomp'yutinga [Models and methods of automatic classification of objects by features based on immunocomputing], *Radioelektronika, informatika, upravlenie* [Radioelectronics, informatics, management], 2010, No. 2, pp. 117-124.

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

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

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