Абстрактная модель искусственной иммунной сети на основе комитета классификаторов и ее использование для распознавания образов клавиатурного почерка

А.Е. Сулавко[1]
[1] *ФГБОУ ВО «Омский государственный технический университет» (ОмГТУ), 644050, г. Омск, просп. Мира, д. 11*

Аннотация

Предложены абстрактная модель искусственной иммунной сети на базе комитета классификаторов и два алгоритма ее обучения (с учителем и с подкреплением) для задач классификации, которые характеризуются малыми объемами и низкой репрезентативностью обучающих выборок. Оценка эффективности модели и алгоритмов выполнена на примере задачи аутентификации по клавиатурному почерку с использованием 3 баз данных биометрических образов. Разработанная искусственная иммунная сеть обладает эмерджентностью, памятью, двойной пластичностью, устойчивостью обучения. Эксперименты показали, что искусственная иммунная сеть дает меньший или сопоставимый процент ошибок по сравнению с некоторыми архитектурами нейронных сетей при гораздо меньшем объеме обучающей выборки.

Ключевые слова: биометрическая аутентификация, бэггинг, бустинг, подпространства признаков, машинное обучение на малых выборках, ансамбли моделей.

Цитирование: **Сулавко, А.Е.** Абстрактная модель искусственной иммунной сети на основе комитета классификаторов и ее использование для распознавания образов клавиатурного почерка // Компьютерная оптика. – 2020. – Т. 44, № 5. – С. 830-842. – DOI: 10.18287/2412-6179-CO-717.

Citation: Sulavko AE. An abstract model of an artificial immune network based on a classifiers committee for biometric pattern recognition by the example of keystroke dynamics. Computer Optics 2020; 44(5): 830-842. DOI: 10.18287/2412-6179-CO-717.

Введение

Один из основных мировых трендов на сегодняшний день связан с развитием технологий искусственного интеллекта (ИИ). Под этим термином подразумевается способность программ выполнять задачи, которые считаются прерогативой человека – классификация, кластеризация, регрессия (аппроксимация функций, прогнозирование временных рядов). Важнейшим свойством для ИИ является возможность *быстрого и устойчивого обучения на малом числе примеров*, что означает способность ИИ обрабатывать большие объемы данных, а также формировать достоверные решения и делать высокоточные предсказания, даже если *обучающая выборка ограничена в объеме и не в полной мере репрезентативна*.

Для решения задач из области ИИ существует множество свободно распространяемых программных продуктов (TensorFlow, Keras, Apache MXNet, ONNX, Chainer, Deeplearning4j, Theano и др), позволяющих сторонним разработчикам использовать методы машинного обучения при создании интеллектуальных приложений. Большинство библиотек машинного обучения базируется на многослойных искусственных нейронных сетях (ИНС). Идеи использования «глубоких» нейросетевых архитектур активно популяризуются, в том числе крупными корпорациями (Google, NVidia, Intel, Microsoft). Во многих случаях эти идеи доведены до эффективных практических решений. Тем не менее, этот аппарат имеет недостатки [1], в частности:

– на небольших выборках итерационные алгоритмы обучения проявляют неустойчивость (склонность к переобучению, падение точности при незначительных изменениях параметров ИНС);

– для настройки многослойных сетей требуется огромная база примеров (десятки, сотни тысяч);

– обучение глубоких нейронных сетей не может быть полностью автоматизировано и всегда ведется под контролем человека (инженер-исследователь вынужден подбирать слишком много параметров, влияющих на структуру нейронной сети и алгоритм обучения, что создает большие трудозатраты);

– известные теоремы о представимости функций в виде ИНС и о сходимости процедур обучения градиентным спуском не дают четкой информации о составлении оптимальной конфигурации ИНС под заданную задачу или обучающую выборку;

– существующие алгоритмы обучения в той или иной степени подвержены проблемам переобучения, затухания градиентов, попадания в локальные минимумы поверхности ошибки, параличей сети.

В настоящей работе рассматривается альтернативный биоинспирированный подход, лишенный указанных недостатков, который может применяться при *ма-*

лых объемах и низкой репрезентативности обучающих выборок. Предложены абстрактная модель искусственной иммунной сети (ИИС) на базе комитета классификаторов и устойчивые алгоритмы ее обучения (с учителем и с подкреплением) для задач классификации.

В работе 2005 года [2] описаны проблемы аппарата ИИС, к которым относится его слабая теоретизация (недостаток строгих доказательств работоспособности, сходимости алгоритмов обучения). Эта проблема остается актуальной в 2020 году [3, 4], хотя работы по расширению доказательной базы ведутся [5]. Настоящее исследование апеллирует к хорошо зарекомендовавшим себя методам построения и обучения ансамблей моделей [6] для усиления формально-теоретической основы предлагаемых решений.

В качестве предметной области для демонстрации эффективности разработанных модели и алгоритмов выбрана задача построения метода биометрической аутентификации субъектов по клавиатурному почерку (индивидуальным особенностям ввода пароля на клавиатуре или мобильном устройстве). Данная задача актуальна в контексте проблем информационной безопасности и относится к трудноразрешимым.

Научная задача и достигнутые ранее результаты

При биометрической аутентификации выполняется сравнение «один к одному» предъявляемого образа и *эталона* определенного субъекта. Для каждого пользователя следует обучать отдельный автомат верификации образов, который настраивается с использованием обучающих выборок (рис. 1) «Свой» (примеры, принадлежащие пользователю) и «Чужие» (примеры, не принадлежащие пользователю).

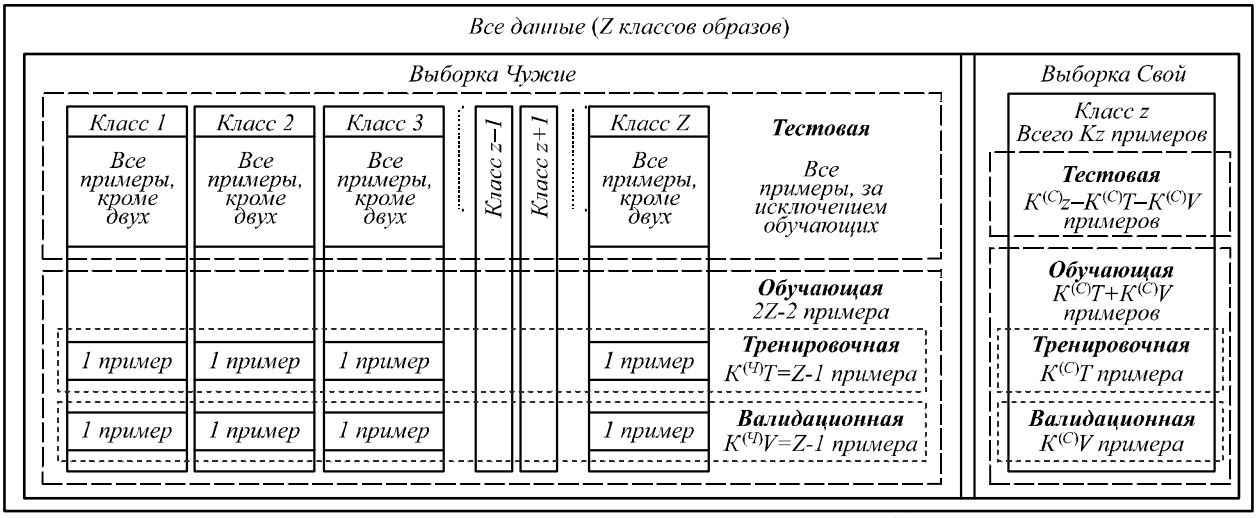

Рис. 1. Структура выборок для испытуемого под номером z, где $к_{T/V}^{(C/Ч)}$ – объем выборки, T – тренировочная, V – валидационная, C – «Свой», Ч – «Чужие», $к^{(C)}=к_T^{(C)}+к_V^{(C)}$

Объем выборки «Свой» в биометрической системе аутентификации ограничен 10 – 30 примерами, обучение должно выполняться за короткий промежуток времени (иначе система не будет востребована на практике). Выборка «Чужие» не ограничена в объеме (можно использовать одну большую выборку «Чужих» для обучения всех автоматов аутентификации).

Обычно биометрические данные предварительно подвергаются обработке, в ходе которой из образца данных удаляется незначимая информация и извлекаются биометрические параметры – *признаки*. При использовании стандартной клавиатуры признаками являются временные задержки нажатий (между нажатиями) клавиш, если для снятия характеристик используется мобильное устройство, то к этим признакам добавляются показатели силы нажатия на экран и площадь соприкосновения пальца с экраном. В настоящей работе использовались базы образов клавиатурного почерка, представленных векторами признаков и не требующие дополнительной обработки.

Признаки клавиатурного почерка малоинформативны и меняются в зависимости от времени суток и психофизиологического состояния человека [7]. Как следствие, обучающая выборка «Свой» оказывается нерепрезентативной. Проблема репрезентативности для выборки «Чужие» остро не стоит.

Вероятность «ложного допуска Чужого» (FAR) должна быть ничтожно мала, а вероятность «ложного отказа Своему» (FRR) может быть выше (приемлемый уровень – 10 – 25 % ошибок). Показатели FRR и FAR взаимозависимы, их соотношение определяет пороговый коэффициент, с помощью которого их можно балансировать. Сравнение методов распознавания иногда осуществляется по средней точности (Mean Accuracy, далее $MAC = 1 - (FRR + FAR)/2$) – соотношению верных решений и количества опытов. Однако чаще используется коэффициент равной вероятности ошибок EER, когда выполняется условие: $EER \approx FAR \approx FRR \approx 1 - MAC$. Для этого при тестировании строятся характеристические кривые (ROC-кривые), отображающие взаимную зависимость FRR, FAR и порогового коэффициента. Если MAC принимает низкие значения, например, менее 0,9 (или $EER > 0{,}1$), то, настроив систему на $FAR = 0{,}0001$, мы

можем получить $1 \geq FRR > 0{,}5$ (более 50 % «ложных отказов»). Все зависит от характера ROC-кривых.

Достигнутые ранее результаты (табл. 1) говорят о том, что найти решение этой задачи затруднительно, в том числе в нейросетевом логическом базисе. Для использования потенциала методов «глубокого» обучения требуется большой объем обучающей выборки, не реализуемый на практике (320 примеров на человека). Рассматриваемая научная задача хорошо иллюстрирует ограниченность применимости ИНС.

Табл. 1. Достигнутые показатели надежности для методов классификации субъектов по клавиатурному почерку

Сведения о методе классификации	Объем обучающей выборки «Свой» $\kappa^{(C)}$ (на человека)	Описание базы данных образов	EER	MAC
			в долях / вероятностях	
Рекуррентные ИНС (2 LSTM блока, оптимизатор Adam) [8]		**Б1 (n = 31)**: 51 испытуемый (по 400 примеров ввода пароля ".tie5Roanl" на клавиатуре, всего 20400 образов), данные получены за 6 месяцев (испытуемые вводили по 50 примеров через определенный период времени) [10]	0,227	0,773
Рекуррентные ИНС (3 GRU блока, оптимизатор Adam) [8]			0,15	0,85
Рекуррентные ИНС (3 LSTM блока, оптимизатор Adam) [8]			0,219	0,781
Малые и «глубокие» сверточные ИНС с предобучением и без [9]	200 –300			**≤ 0,925**
«Манхэттенская» масштабируемая метрика [10]	200 примеров		**0,096**	**0,904**
Меры Махаланобиса и ближайшего соседа [10]	200 примеров		0,10	0,9
Статистическая техника (на базе z-оценки) [10]	200 примеров		0,102	0,898
Машина опорных векторов (SVM) [10]	200 примеров		0,102	0,898
Автоассоциативный многослойный персептрон [10]	200 примеров		0,161	0,839
Мера Евклида [10]	200 примеров		0,215	0,785
Нечеткая логика [10]	200 примеров		0,221	0,779
Метод k-ближайших соседей (k-NN) [10]	200 примеров		0,372	0,628
«Глубокая» ИНС, оптимизатор Nadam [11]	320 примеров			**0,92**
SVM [11]	320 примеров			0,7115
Наивный Байес [12]	34 примера	**Б2 (n = 71)**: 42 испытуемых (по 51 примеру ввода ".tie5Roanl" на планшете или смартфоне), данные временных задержек, силы нажатия, площади касания [12]		0,7893
Сети Байеса [12]	34 примера			0,9194
C4.5 (J48) [12]	34 примера			0,6902
k-NN [12]	34 примера			0,7298
SVM [12]	34 примера			0,8833
Случайный лес [12]	34 примера			**0,9304**
Многослойный персептрон [12]	34 примера			0,8626
Мера Евклида [12]	34 примера		0,157	0,843
«Манхэттенская» метрика [12]	34 примера		**0,129**	**0,871**
Мера Махаланобиса [12]	34 примера		0,166	0,834

Архитектура клеток иммунной сети

Прежде всего, отметим, что ИИС (как и ИНС) – крайне упрощенная конструкция, которая не подразумевает строгого соответствия своему биологическому прототипу. Искусственные иммунные системы (сети) в компьютерных науках принято рассматривать как семейство алгоритмов [4], основанных на соответствующих теориях о естественной иммунной системе (ЕИС): дендритных клеток, негативного отбора, клональной селекции (положительного отбора), сетевых алгоритмов (последние чаще всего называют иммунными сетями, а не системами, далее все типы иммунных моделей будем называть ИИС).

Иммунная система содержит множество клеток (макрофаги, дендритные клетки, лимфоциты), которые обладают способностью обнаруживать и удалять чужеродные организмы (антигены). Назовем все такие клетки *детекторами* [4] – вычислительными элементами, способными анализировать распознаваемый образ либо его отдельные фрагменты и реагировать на него пропорционально тому, насколько этот образ соответствует антигену. Шкала реакций задана на интервале действительных чисел [0; 1], где 0 – полная уверенность в том, что клетка принадлежит организму (гипотеза «Свой»), а 1 – полная уверенность в обратном (гипотеза «Чужой»). Силу взаимодействия между клетками ИИС и антигеном также называют *аффинностью*. Каждый детектор следует рассматривать как бинарный классификатор, состоящий из нескольких функций, последовательно применяющихся к биометрическому образу. Образ представляет собой вектор признаков фиксированной длины $\bar{a} = \{a_1, a_2, \ldots, a_n\}$, где n – количество признаков, которое должно присутствовать в образе. В общем виде получение реакции i-го детектора на входной образ $\bar{a}$ можно описать формулой (1):

$$u_i = \varphi_\chi\left(y' = \phi\left(y = f_x(\bar{\alpha} = R(\bar{a}, \Psi_i), \breve{g}, \Theta_i), \mathrm{T}_i\right)\right), \quad (1)$$

опишем функции детектора и их параметры:

1) $\bar{\alpha} = R(\bar{a}, \Psi_i)$ – функция-рецептор, предоставляющая интерфейс взаимодействия для детектора и антигена. Данная функция извлекает η из n признаков, содержащихся в $\bar{a}$, Ψ_i – множество номеров признаков из $\bar{a}$, которые должен анализировать i-й детектор. Вектор $\bar{\alpha} = \{a_1, a_2, \ldots, a_\eta\}$ является подмножеством $\bar{a}$ с собственной сквозной нумерацией элементов;

2) $y=f_x(\bar{\alpha},\breve{g},\Theta_i)$ – функция-ядро детектора, параметрический функционал, который вычисляет близость вектора $\bar{\alpha}$ к эталону класса образов «Свой»; x – тип функционала (ниже даны формулы (2 – 11)); $\breve{g}$ – вектор параметров функционала, которые влияют на характер вычислений; $\Theta_i=\{\mu_1,\mu_2,\ldots,\mu_\eta,\sigma_1,\sigma_2,\ldots,\sigma_\eta\}$, μ_j и σ_j – статистические оценки параметров распределения значений j-го признака из вектора $\bar{\alpha}$. Данные из множества Θ_i рассчитываются на основании нескольких случайных примеров из обучающей выборки (далее *фолд*). В настоящей работе для построения ядер детекторов применялись следующие функционалы: мера Минковского (2), разные вариации меры Байеса–Минковского (3 – 5), «наивный Байес» в дифференциальной (6) и интегральной форме (7), параметрические критерии (8 – 11). Разные функционалы образуют различные виды детекторов, которые дают слабо коррелированные решения относительно друг друга. Из любого функционала можно получить разные меры близости за счет изменения параметров $\breve{g}$. Часть представленных мер близости применялась в работе [13] при построении «гибких» нейронных сетей.

$$f_1(\bar{\alpha},\breve{g}=\{g\},\Theta_i)=\sqrt[g]{\sum_{j=1}^{\eta}\left|\frac{(\mu_j-a_j)}{\sigma_j}\right|^g}, \quad (2)$$

$$f_2(\bar{\alpha},\breve{g}=\{g\},\Theta_i)=\sum_{j=1}^{\eta}\left|\left|\frac{(\mu_t-a_t)}{\sigma_t}\right|^g-\left|\frac{(\mu_j-a_j)}{\sigma_j}\right|^g\right|, \quad (3)$$

$$f_3(\bar{\alpha},\breve{g}=\{g\},\Theta_i)=\sqrt[g]{\sum_{j=1}^{\eta}\left|\left|\frac{(\mu_t-a_t)}{\sigma_t}\right|^g-\left|\frac{(\mu_j-a_j)}{\sigma_j}\right|^g\right|}, \quad (4)$$

$$f_4(\bar{\alpha},\breve{g}=\{g\},\Theta_i)=\sqrt[g]{\sum_{j=1}^{\eta}\left|\frac{a_t}{\sigma_t}-\frac{a_j}{\sigma_j}\right|^g}, \quad (5)$$

где a_j – значение j-го признака, μ_j и σ_j – математическое ожидание и среднеквадратичное отклонение j-го признака, g – степенной коэффициент, $g\in[0{,}01;100]$. Мера Минковского ориентирована на нахождение расстояния в пространстве признаков с низким уровнем взаимной корреляционной зависимости $r_{j,t}<0{,}5$ (где $r_{j,t}$ – коэффициент парной корреляции Пирсона между j-м и t-м признаками). Когда признаки независимы ($r_{j,t}\approx 0$), оптимальное значение степенного коэффициента $g=2$ (мы имеем меру Пирсона, а при $\sigma_j=1$ – меру Евклида). При $g=1$ мы получаем меру «городских кварталов», при $g\to\infty$ мера Минковского стремится к мере Чебышева. Если пространство признаков искривлено из-за корреляционных связей между признаками ($0>r_{j,t}<0{,}5$), то изменение g позволит выполнять более точное вычисление расстояний Минковского. Мера Байеса–Минковского, напротив, ориентирована на обработку сильно зависимых признаков ($r_{j,t}>0{,}5$). Изменение g позволяет давать более точную оценку близости при разных уровнях взаимной коррелированности признаков. Желательно подбирать признаки Ψ_i таким образом, чтобы коэффициенты парной корреляции $r_{j,t}$ были близки по значению [1], причем для меры Минковского $r_{j,t}<0{,}5$, а для меры Байеса–Минковского $r_{j,t}>0{,}5$.

$$f_5(\bar{\alpha},\breve{g}=\{g_1,g_2,\ldots,g_\eta\},\Theta_i)=\prod_{j=1}^{\eta}p_{g_j}(a_j,\mu_j,\sigma_j), \quad (6)$$

$$f_6(\bar{\alpha},\breve{g}=\{g_1,g_2,\ldots,g_\eta\},\Theta_i)=\prod_{j=1}^{\eta}P_{g_j}(a_j,\mu_j,\sigma_j), \quad (7)$$

где $P_g(a,\mu,\sigma)$ и $p_g(a,\mu,\sigma)$ – значение функции распределения и плотности вероятности соответственно, с учетом значения признака a_j и его параметров распределения (μ_j и σ_j) для класса «Свой». Реализация этих функций зависит от закона распределения, который определяется параметром g_j. В настоящей работе использовалось три вида закона распределения:

– *нормальный* ($g_j=1$):

$$p_1(a_j,\mu_j,\sigma_j)=\frac{1}{\sigma_j\sqrt{2\pi}}e^{-\frac{(a_j-\mu_j)^2}{2\sigma_j^2}},$$

$$P_1(a_j,\mu_j,\sigma_j)=\frac{1}{\sigma_j\sqrt{2\pi}}\int_{\mu_j-5\sigma_j}^{a_j}e^{-\frac{(\vartheta-\mu_j)^2}{2\sigma_j^2}}d\vartheta,$$

где μ_j и σ_j – математическое ожидание и среднеквадратичное отклонение j-го признака;

– *логнормальный* ($g_j=2$):

$$p_2(a_j,\mu_j,\sigma_j)=\frac{1}{a_j\sigma_j\sqrt{2\pi}}e^{-\frac{(Ln(\vartheta)-\mu_j)^2}{2\sigma_j^2}},$$

$$P_2(a_j,\mu_j,\sigma_j)=\frac{1}{a_j\sigma_j\sqrt{2\pi}}\int_{\mu_j-5\sigma_j}^{a_j}e^{-\frac{(Ln(\vartheta)-\mu_j)^2}{2\sigma_j^2}}d\vartheta,$$

где μ_j и σ_j – параметр масштаба и формы;

– закон распределения *Лапласа* ($g_j=3$):

$$p_3(a_j,\mu_j,\sigma_j)=\frac{\sigma_j}{2}e^{-\sigma_j|a_j-\mu_j|},$$

$$P_3(a_j,\mu_j,\sigma_j)=\begin{cases}0{,}5e^{\sigma_j(a_j-\mu_j)}, a_j\le\mu_j\\ 1-0{,}5e^{-\sigma_j(a_j-\mu_j)}, a_j>\mu_j\end{cases},$$

где μ_j и σ_j – коэффициенты сдвига и масштаба.

Параметры клавиатурного почерка, а также большинство других биометрических признаков имеют законы распределения, близкие к указанным выше [14]. При решении иных задач распознавания образов перечень законов распределения может быть расширен.

$$f_7(\bar{\alpha},\breve{g}=\{g\},\Theta_i)=\\ =\int_{-5}^{5}\sqrt[g]{|P_1(\vartheta,\mu_a,\sigma_a)-P_1(v,0,1)|^g}\cdot d\vartheta, \quad (8)$$

$$f_8(\bar{\alpha},\breve{g}=\{g\},\Theta_i)= \\ =\int_{-5}^{5}\sqrt[g]{|\,p_1(\vartheta,\mu_{\hat{a}},\sigma_{\hat{a}})-p_1(\vartheta,0,1)\,|^g}\cdot d\vartheta, \quad (9)$$

$$f_9(\bar{\alpha},\breve{g}=\{g\},\Theta_i)= \\ =\int_{-5}^{5}\sqrt[g]{|\,P_1(\vartheta,\mu_{\hat{a}},\sigma_{\hat{a}})\cdot(1-P_1(\vartheta,0,1))\,|^g}\cdot d\vartheta, \quad (10)$$

$$f_{10}(\bar{\alpha},\breve{g}=\{g\},\Theta_i)= \\ =\int_{-5}^{5}\sqrt[g]{|\,p_1(\vartheta,\mu_{\hat{a}},\sigma_{\hat{a}})\cdot p_1(\vartheta,0,1)\,|^g}\cdot d\vartheta. \quad (11)$$

Последняя группа функционалов (8 – 11) представляет собой модификации критериев согласия, используемых для сравнения эмпирически наблюдаемой функции распределения (плотности вероятности) для величины $\hat{a}$ с теоретической (эталонной), при этом предполагается, что закон распределения близок к нормальному, $\hat{a}$ – нормированное значение любого признака, $\mu_{\hat{a}}$ и $\sigma_{\hat{a}}$ – математическое ожидание и среднеквадратичное отклонение. Нормирование (приведение всех a_j к единой случайной величине $\hat{a}$) производится по данным из Θ_i в соответствии с формулой:

$$\dot{a}=\frac{a_j-\mu_j}{\sigma_j}.$$

Параметры распределения $\hat{a}$ для класса «Свой» должны принимать стандартные значения ($\mu_{\hat{a}}\approx 0$ и $\sigma_{\hat{a}}\approx 1$), для образов «Чужих» будут наблюдаться значительные отклонения ($\mu_{\hat{a}}\neq 0$ и/или $\sigma_{\hat{a}}>1$). Предложенные функционалы (8 – 11) обобщают критерии Джини, среднего геометрического вероятности и плотности вероятности, рассмотренные в работах [15, 16];

3) $y'=\varphi(y, T_i)$ – функция нормирования откликов y относительно порога T_i, который вычисляется в процессе настройки i-го детектора. Функция нормирования может иметь 2 реализации:

$$\varphi(y, T_i)=y/T_i,$$

если y – это расстояние от $\bar{\alpha}$ до эталона класса «Свой» (чем меньше, тем ближе), тогда T_i – это максимальное значение функции-ядра i-го детектора, при поступлении на его вход обучающих образов «Свой», либо:

$$\varphi(y, T_i)=T_i/y,$$

если y – это вероятность того, что $\bar{\alpha}$ принадлежит классу «Свой», тогда T_i – это минимальное значение функции-ядра i-го детектора, при поступлении на его вход обучающих образов «Свой». Физический смысл y (расстояние или вероятность) зависит от функции-ядра соответствующего детектора (например, для меры Евклида требуется использовать первый вариант, а для «наивного Байеса» – второй);

4) $u_i=\phi_\chi(y'_i)$ – функция активации, дополнительный нелинейный элемент детектора, который определяет особенности реагирования на антиген. Функция активации также необходима, чтобы привести отклик детектора к области значений [0; 1]. В настоящей работе применялись сигмоиды (арктангенс, гиперболический тангенс и др.). В качестве функций активации имеет смысл использовать либо наиболее быструю из сигмоидальных, либо применять функции, которые дают как можно более отличающиеся результаты, чтобы создавать детекторы с низкой коррелированностью решений на базе однотипных мер близости (в целом x в большей степени влияет на характер преобразований (1) детектора, чем χ).

Одной из теоретических проблем аппарата ИИС является слабая обоснованность используемых мер близости [2] (чаще всего применяется мера Евклида). Согласно теореме «об отсутствии бесплатных завтраков» (No Free Lunch) ни одна мера близости не может быть оптимальной для всего множества задач распознавания образов. Поэтому в настоящей работе каждый детектор определяет аффинность уникальным способом, а состав детекторов «подстраивается» под задачу и определяется в процессе обучения ИИС.

Искусственная иммунная сеть как система двух комитетов классификаторов

Предлагается разделить детекторы на две группы: врожденный и приобретенный иммунитет, и рассматривать их как *два комитета (ансамбля)* слабых классификаторов, обучаемых при помощи разных алгоритмов. Коллективное решение комитета из N детекторов может быть вычислено как среднее частных решений:

$$\ddot{u}=\Phi(\bar{D}^*=\{D_1^*,\ldots D_N^*\},\bar{a})= \\ =\frac{1}{N}\cdot\sum_{i=1}^{N}\varphi(D_i^*,\bar{a})=\frac{1}{N}\cdot\sum_{i=1}^{N}u_i.$$

Врожденный иммунитет (ВИ) передается посредством генов, органы иммунной системы формируются еще при эмбриональном развитии. У эмбрионов В-лимфоциты образуются в печени и костном мозге. В предлагаемой модели костный мозг является местом пребывания иммунокомпетентных детекторов, параметры и состав которых определяются в ходе эмбрионального (и постэмбрионального) развития. Так, ВИ формируется в процессе итерационного обучения ИИС с использованием *тренировочной* и *валидационной* выборок (рис. 2). Последняя используется для промежуточной оценки надежности решений ИИС при смене поколения детекторов (схожие практики применяются при обучении ИНС). Обе выборки являются *непересекающимися* подмножествами *обучающей* выборки (рис. 1).

Приобретённый иммунитет (ПИ) развивается с течением жизни и определяет способность организма обезвреживать специфические антигены, которые попадали в организм ранее. В формировании ПИ участ-

вует тимус – орган, в котором происходит созревание и обучение Т-лимфоцитов. В предложенной модели тимус осуществляет настройку и отбор иммунокомпетентных детекторов, используя валидационную выборку. Адаптивный иммунный ответ приводит к появлению иммунологических клеток памяти (представленных в ИИС детекторами), которые долгое время пребывают в «спящем состоянии» до повторной встречи с тем же антигеном. В разработанной модели ИИС приобретенный иммунитет формируется в процессе функционирования ИИС. Если решение об отнесении образа к категории «Свой» или «Чужой» является неоднозначным, могут генерироваться новые иммунокомпетентные детекторы.

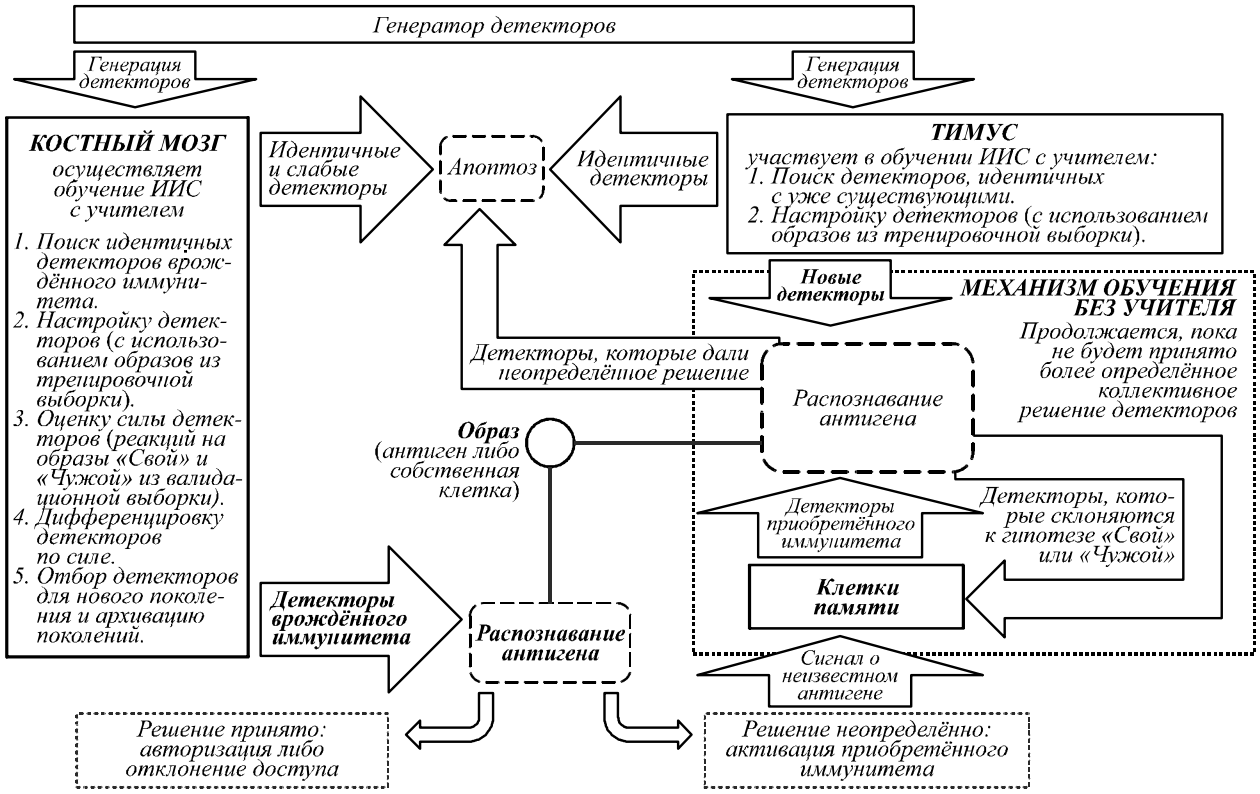

Рис. 2. Функциональная схема ИИС

Идея объединения классификаторов в комитет основана на теореме Кондорсе, которая утверждает: если мнения экспертов независимы и вероятность правильного решения каждого из них больше 0,5, то с увеличением количества экспертов вероятность правильного решения комитета экспертов возрастает и стремится к единице. Причем чем выше вероятность верного решения для каждого эксперта в отдельности, тем выше вероятность верного решения комитета. Отметим, что решение любого детектора можно инвертировать, чтобы преодолеть барьер Кондорсе в 0,5 (известны также доказательства других теорем [17], позволяющих обойти барьер Кондорсе).

Однако на практике решения классификаторов, играющих роль экспертов, в той или иной мере коррелированы. Чем ниже коррелированность решающих правил, тем более ощутим положительный эффект при их комплексировании. Таким образом, имеются следующие *гиперпараметры*, которые влияют на эффективность комитета детекторов:

– N – количество детекторов;

– RD – матрица коэффициентов корреляции Пирсона $r(\bar{u}_i, \bar{u}_l)$ между решениями всех возможных пар детекторов, где $\bar{u}_i$ – вектор реакций i-го детектора на примеры образов «Чужих» из тренировочной или валидационной выборки;

– Δu – сила детекторов, их способность давать как можно более высокие показатели разницы средних уровней реакции на образы «Свой» и «Чужой» (12):

$$\Delta u = \mu_u^{(Ч)} - \mu_u^{(С)}, \quad \mu_u^{(Ч)} > \mu_u^{(С)}. \tag{12}$$

В рамках предыдущих исследований [18] была апробирована стратегия снижения уровня коррелированности решений детекторов, которая оказалась недостаточно продуктивной. Процедура оценки показателей $r(\bar{u}_i, \bar{u}_l)$ и дифференциации по ним детекторов оказалась ресурсоемкой. Кроме того, не наблюдалось сходимости алгоритма настройки ИИС. Процесс обучения был слишком длительным и не всегда приводил к ожидаемому результату (не всегда удавалось найти N детекторов с заданным минимальным уровнем взаимной коррелированности решений). По этой причине в настоящей работе выбрана стратегия повышения силы детекторов при условии, что они не должны быть идентичными. При появлении в ИИС идентичных или слабых детекторов происходит

апоптоз – процесс программируемой клеточной гибели для уничтожения дефектных клеток (рис. 2).

Необходимо, чтобы решения всех детекторов врожденного и приобретенного иммунитета не являлись полностью коррелированными. Поэтому после генерации детектора должна осуществляться проверка идентичности параметров нового детектора и уже существующих. При обнаружении «двойника» его следует удалить и сгенерировать детектор снова. При этом значения параметров $\breve{g}$ можно считать равными, когда они отличаются менее чем на 10^{-1}. Конечно, решения детекторов будут в той или иной степени коррелированы (но не на 100 %). Чем сильней различаются параметры D_i и D_l, тем менее коррелированы решения i-го и l-го детекторов.

Генерация и настройка детекторов

Детектор можно описать множеством параметров $D_i = \{\Psi_i, \breve{g}, x, \chi\}$. *Сгенерировать детектор* означает сгенерировать данные параметры. Приведем псевдокод функции генерации детектора:

method GenerateDetector(RF)
// RF – матрица парных коэффициентов корреляции
// между признаками
// random(*min*; *max*) – генерация случайного числа
$\eth$ = random(2;n / 2)
r_{max} = random(0,1; 1)
if $r_{max} > 0{,}5$ **then** r_{min} = random(0; r_{max})
else r_{min} = random(0,5; r_{max})
// Выбрать признаки с уровнем взаимной
// корреляции более r_{min}, но менее r_{max}
Ψ_i = GetFeatures(r_{min}; r_{max}; RF)
// Если признаков с заданным уровнем корреляции
// нет, сгенерировать номера признаков снова
if Length(Ψ_i) < η **go to begin**
// Выбор меры близости (Мера Минковского не
// подходит для обработки сильно коррелированных
// признаков, а Байеса-Минковского – для слабо
// коррелированных)
if $r_{max} > 0{,}5$ **then** x = random(2; 10)
else x = random(5; 11)
if x = 11 then x = 1
else
  if $5 \le x \le 6$ **then**
    for j **from** 1 **to** η **do** g_j = random(1; 3) **end**
  else g = random(0,01; 100)
// Выбрать случайную функцию активации
X = GetRandomActivationFunction( )
$D_i = \{\Psi_i, \breve{g}, x, \chi\}$
// Если новый детектор идентичен одному из
// детекторов ВИ или ПИ, то сгенерировать заново
if IsIdenticalToExisting(D_i) = true **then**
  D_i = GenerateDetector(RF)
return D_i

В разработанной ИИС реализуется идея *случайных подпространств признаков*, но в отличие от алгоритма «случайный лес» Ψ_i задается с учетом корреляции между признаками. Этот прием называется *симметризацией корреляционных связей* [19].

Другая идея, которая реализована при генерации детекторов, заключается в объединении разнородных *случайных классификаторов* (например, описывая признак разными законами распределения, можно получить несколько «наивных» классификаторов Байеса, решения которых не полностью коррелированы). Примером подобной техники является нейросетевое обобщение множества различных критериев [15].

Настройка детектора связана с вычислением порога T_i и эталонных описаний признаков Θ_i (μ_j и σ_j).

Настроенный детектор можно обозначить как $D^*_i = \{\Psi_i, \breve{g}, x, \chi, \Theta_i, T_i\}$, а функцию (1) – как $\phi(D^*_i)$.

Алгоритм обучения иммунной сети с учителем (формирование врожденного иммунитета)

Известны следующие базовые методы и подходы для обучения ансамблей моделей:

1. Бэггинг (bootstrap aggregating) – метаалгоритм композиционного обучения машин, основная идея которого заключается в обучении базовых (слабых) классификаторов на разных подмножествах обучающей выборки. Базовые классификаторы могут быть идентичными или иметь разные архитектуры. Бэггинг уменьшает дисперсию голосов базовых классификаторов и помогает избежать переобучения. Принцип работы бэггинга схож с принципами работы метода случайных классификаторов, а также методов накопления сигналов при их обнаружении и заключается в повышении отношения сигнал / шум.
2. Бустинг (boosting) – семейство алгоритмов машинного обучения, преобразующих слабые обучающие алгоритмы к сильным. Бустинг строит ансамбль путём тренировки каждого нового классификатора, уделяя больше внимания обучению на тех тренировочных примерах, которые предыдущие модели классифицировали ошибочно (например, путем присвоения весов обучающим примерам), и имеет тенденцию к переобучению. Эффективность этого подхода доказана экспериментально и теоретически, что впервые подтверждено для алгоритма AdaBoost [20].
3. Стекинг (stacked generalization) предполагает построение многослойных структур из ансамблей классификаторов, когда выходные данные ансамбля первого слоя воспринимаются ансамблем второго слоя как входные данные (метапризнаки). При использовании стекинга увеличивается необходимый для обучения объем выборки, так как для корректного обучения метамодели каждый слой требуется настраивать на разных тренировочных примерах.

При разработке итерационного алгоритма обучения ИИС были учтены первые два подхода (бэггинг позволяет компенсировать склонность к переобучению бустинга), но от стекинга решено отказаться,

учитывая малый объем обучающей выборки, а также тот факт, что ИИС не образует конструкций в виде слоев.

В разработанном алгоритме на каждой итерации происходит генерация новой популяции детекторов, которые настраиваются с учетом нескольких случайных тренировочных примеров (бэггинг), и выполняется промежуточная оценка их эффективности как на тренировочной, так и на валидационной выборке (рис. 3), слабые детекторы уничтожаются (апоптоз), в результате появляется новое поколение иммунокомпетентных (более эффективных) детекторов. Мерой эффективности (обученности) детекторов можно считать Δu (12). По результатам последней валидации вычисляются оценки $\mu_u^{(C)}$ и $\mu_u^{(Ч)}$ для коллективного решения детекторов ВИ. Эти параметры используются для построения *интервала неопределенности решения (ИНР)* $[\mu_u^{(C)}; \mu_u^{(Ч)}]$. ИНР является частью механизма подкрепления при дообучении ИИС в процессе функционирования. Этот механизм активируется при формировании ПИ, что будет изложено в следующем параграфе.

На каждой итерации обучения синтезируются новые образы «Чужих» (рис. 3) путем скрещивания тренировочных примеров, которые хуже всего классифицируются детекторами ВИ (далее сильные «Чужие»). Сильные «Чужие» дают наименьшую среднюю совокупную реакцию детекторов $\ddot{u}$. Скрещивание образов $\bar{a}_k$ и $\bar{a}_m$ происходит с помощью линейной интерполяции значений признаков:

$$a_{c,j} = \frac{C_{syn}+1-c}{C_{syn}+1}\cdot a_{k,j} + \frac{c}{C_{syn}+1}\cdot a_{m,j},$$

где C_{syn} – количество синтетических примеров, порождаемых парой «сильных Чужих» предыдущего поколения (в настоящей работе $C_{syn}=1$), c – номер синтетического примера, j – номер признака. Этот способ синтеза «Чужих» наиболее эффективен, если значения признаков имеют распределения, близкие к нормальному, на нем основан ГОСТ Р 52633.2-2010, имеющий отношение к тестированию средств высоконадежной биометрической аутентификации.

Синтетические образы, получаемые путем скрещивания сильных «Чужих», добавляются в тренировочную выборку. Детекторы нового поколения настраиваются с учетом синтезированных примеров, что позволяет следующему поколению детекторов лучше классифицировать образы «Чужих», наиболее близких к образам «Свой». Таким образом, *ИИС одновременно «учится» создавать образы более сильных «Чужих» и распознавать их. Предложенный механизм размножения сильных «Чужих» при обучении является еще одной вариацией бустинга.*

На скорость и эффективность алгоритма обучения, представленного на рис. 3, более всего влияют следующие основные параметры:

$I_{ВИ}$ – количество итераций обучения (валидаций);

$N_{ВИ}$ – количество детекторов ВИ;

Q – количество сильных «Чужих» (на каждой итерации генерируется $C_{syn}\cdot Q(Q-1)/2$ примеров).

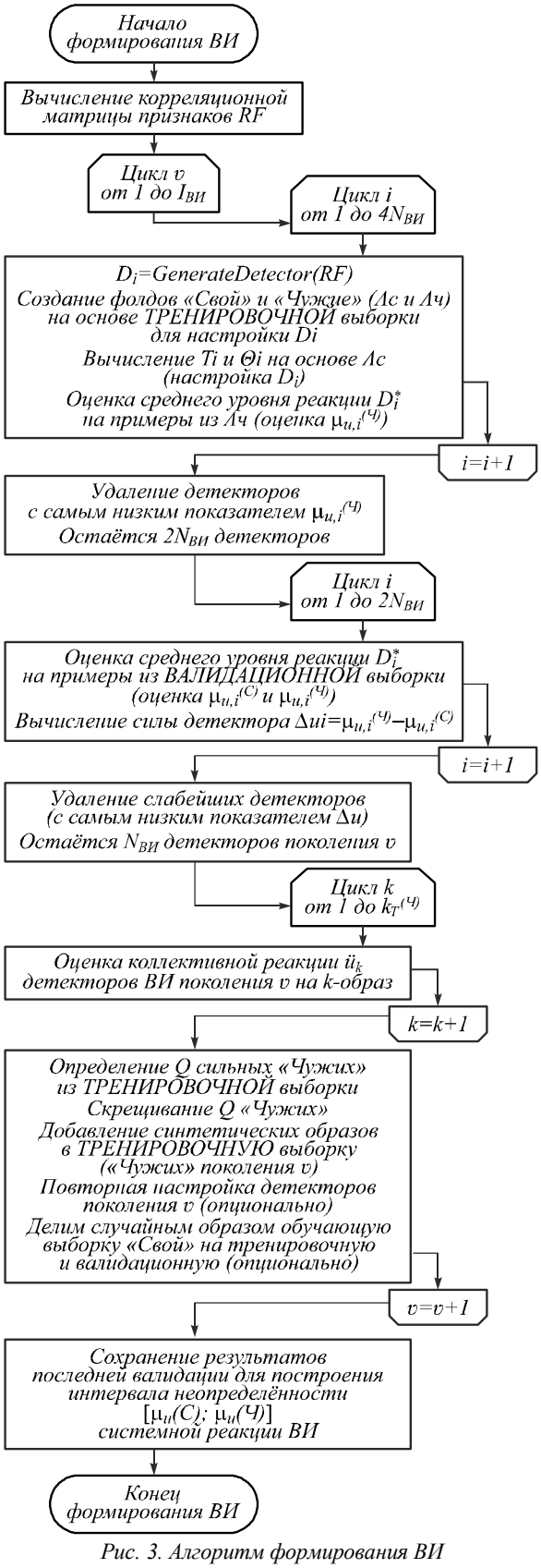

Рис. 3. Алгоритм формирования ВИ

Также параметрами алгоритма являются объемы тренировочной (κ_T) и валидационной выборок (κ_V), размеры фолдов «Свой» ($\kappa_F^{(C)}$) и «Чужой» ($\kappa_F^{(Ч)}$). В настоящем исследовании размер фолдов определялся из соотношения $\kappa_F^{(Ч)} = \kappa_T^{(Ч)} / 3$, $\kappa_F^{(C)} = 2 \cdot \kappa_T^{(C)} / 3$. Объем тренировочной выборки «Чужие» и размер фолда «Чужие» не являются фиксированными, а увеличиваются с каждой итерацией обучения при добавлении в тренировочную выборку *синтетических примеров*. Валидационная выборка всегда остается неизменной.

Алгоритм дообучения иммунной сети с подкреплением (формирование приобретенного иммунитета)

Если обучающая выборка нерепрезентативна, эффективность детекторов ВИ может не соответствовать оценке Δu (12), при этом нет гарантий, что плохо настроенные детекторы в действительности преодалевают барьер Кондорсе (для таких детекторов оценки на тестовой выборке должны принимать вид $\mu_{u,i}^{(Ч)} < \mu_{u,i}^{(C)}$). Обойти барьер Кондорсе можно, если дать возможность детекторам ПИ голосовать за коллективное решение детекторов ВИ.

Введем следующее правило, основанное на ИНР: при $u_i > \mu_u^{(Ч)}$ или $u_i < \mu_{u,i}^{(C)}$ решение D^*_i считается определенным, а при $\mu_u^{(C)} < u_i < \mu_u^{(Ч)}$ решение D^*_i не определено. Если при распознавании образа решение детекторов ВИ считается неопределенным, то активируется механизм ПИ (рис. 4). Генерируются новые детекторы, которые настраиваются на других данных – примерах из валидационной выборки. Для новых детекторов вычисляются реакции u_i, но при формировании коллективного решения учитываются голоса только тех детекторов, которые дают определенный ответ (эти детекторы становятся клетками памяти), детекторы ПИ с неопределенным ответом уничтожаются. На скорость и эффективность алгоритма дообучения, представленного на рис. 4, более всего влияют следующие основные параметры:

$I_{ПИ}$ – количество итераций обучения;

$N_{ПИ}^{(max)}$ – максимальное количество детекторов ПИ (тогда $N_{ПИ}$ – их фактическое количество).

Введение $I_{ПИ}$ позволяет избежать бесконечного цикла дообучения. Детекторы приобретенного иммунитета могут компенсировать недостаток априорных знаний о классах образов «Свой» и «Чужой».

Результаты эксперимента

Для проверки эффективности предложенных модели и алгоритмов использовалось 3 базы клавиатурного почерка: из работ [10] (Б1), [12] (Б2) (см. табл. 1) и собственная база (Б3). Последняя включает 32 человека, каждый из которых 50 раз ввел на клавиатуре фразу «система защиты должна постоянно совершенствоваться» ($n = 63$, учтены только попытки безошибочного ввода).

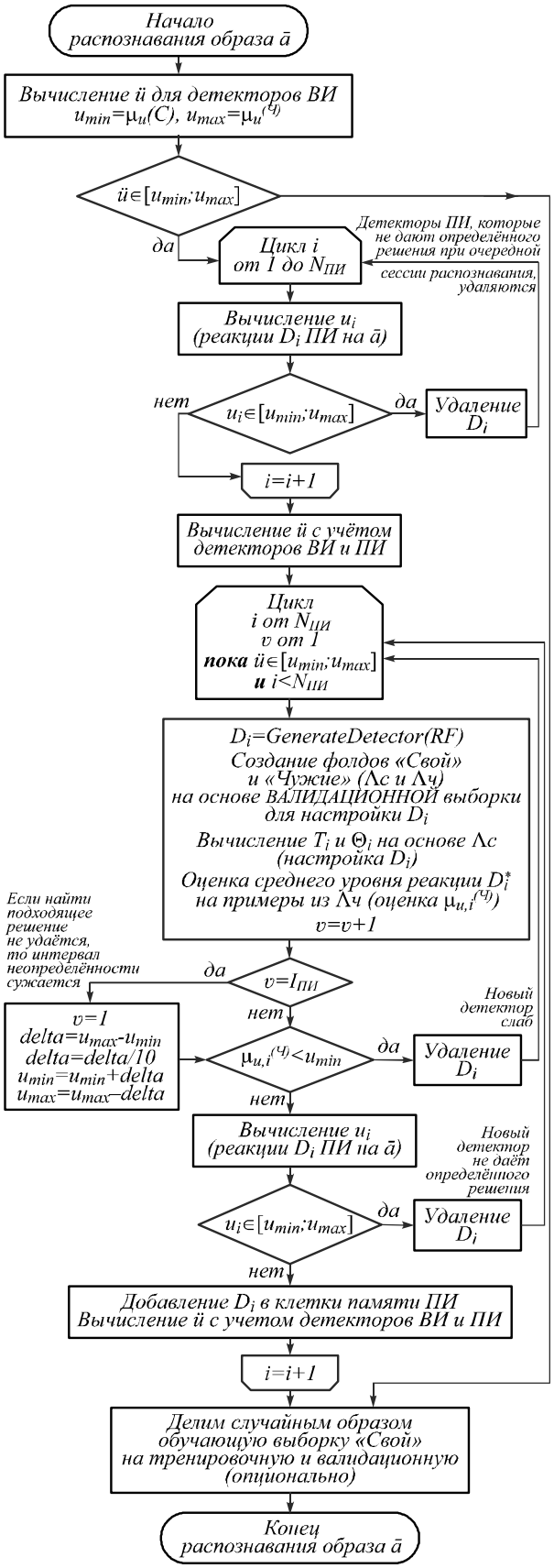

Рис. 4. Алгоритм работы ПИ

Опыты проводились при различном объеме обучающей выборки примеров «Свой»: от $\kappa^{(C)} = 20$ до

$\kappa^{(C)}=40$. Тренировочная $\kappa_T^{(C)}$ и валидационная $\kappa_V^{(C)}$ выборки примеров «Свой» (подмножества обучающей) перед обучением делились в соотношении: $\kappa_T^{(C)}=2\cdot\kappa_V^{(C)}$. Тренировочная $\kappa_T^{(Ч)}$ и валидационная $\kappa_V^{(Ч)}$ выборки примеров «Чужих» включали по одному примеру от каждого испытуемого из набора данных, кроме примеров «Свой» (рис. 1). Остальные примеры использовались в качестве текстовой выборки. Тестирование проводилось методом перекрёстного сравнения (при расчете FAR образ каждого субъекта сравнивался с эталонами всех остальных субъектов). Таким образом, для каждого испытуемого объем тестовой выборки «Чужих» варьировался в зависимости от набора данных так: Б1 – 19900, Б2 – 1968, Б3 – 1488. Показатели FRR и FAR вычислялись как отношение числа ошибок «ложного отказа» или «ложного доступа» к числу соответствующих опытов. Результаты представлены на рис. 5 и в табл. 2.

Рис. 6 иллюстрирует, как определить EER, а также что FRR и FAR можно балансировать, например FRR = 0,193 при FAR = 0,0001 (рис. 6*б*).

Надежность решений зависит от того, как была составлена обучающая выборка. Это наглядно видно при тестировании на базе Б1 [10], которая отсортирована по временным меткам. Если выбирать обучающие примеры равномерно (как в [11], где MAC = 92,6), то обучающая выборка будет репрезентативной, но если обучать и тестировать систему на образах испытуемого, которые были введены в разные дни (с большим перерывом), то репрезентативность выборки окажется низкой. В этом случае наблюдается более существенная разница в надежности решений для режима ВИ (когда используются детекторы только врожденного иммунитета, т.е. $N_{ПИ}^{(max)}=0$) и ВИ+ПИ (когда используются детекторы врожденного и приобретенного иммунитета, т.е. $N_{ПИ}^{(max)}>0$).

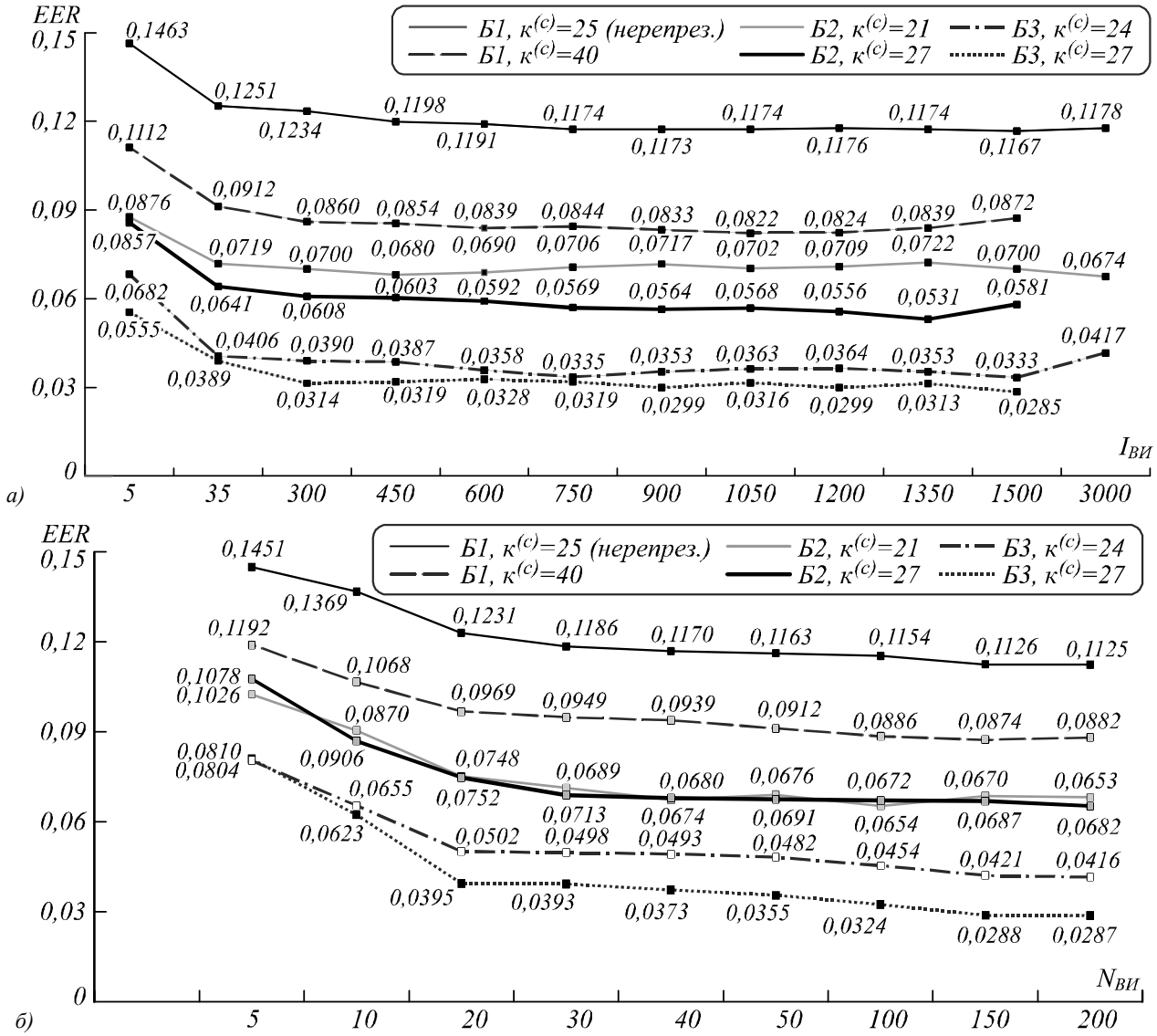

Рис. 5. ROC-кривые, демонстрирующие результаты эксперимента при использовании только врожденного иммунитета ($N_{ПИ}^{(max)}=0$) при $Q=4$: $N_{ВИ}=50$ (а), $I_{ВИ}=50$ (б)

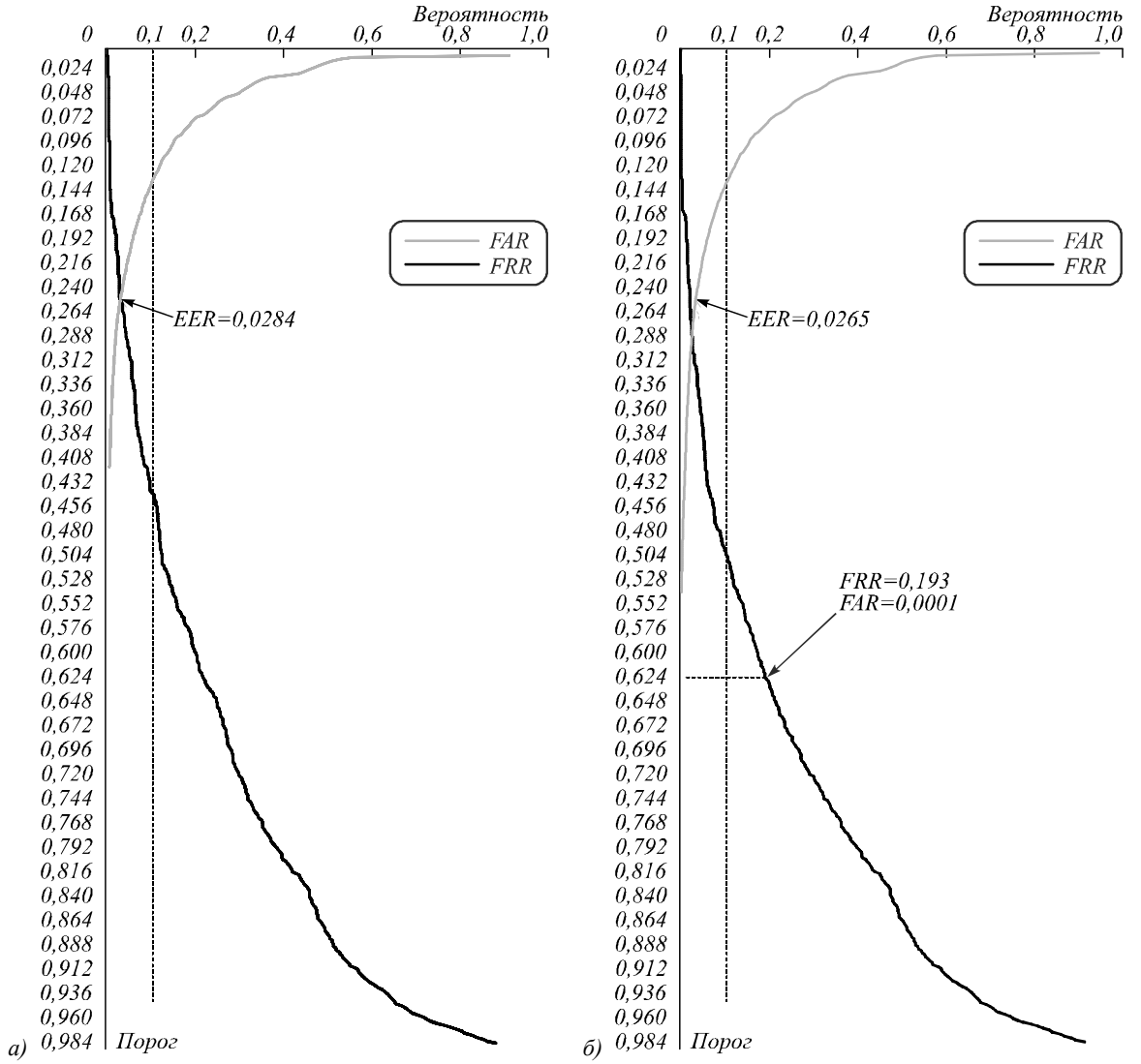

Рис. 6. ROC-кривые, демонстрирующие результаты эксперимента для Б3, при $Q = 4$, $I_{ВИ} = 1500$, $\kappa^{(C)} = 27$: а) ВИ ($N_{ВИ} = 50$, $N_{ПИ}^{(max)} = 0$), б) ВИ + ПИ ($N_{ВИ} = 50$, $N_{ПИ}^{(max)} = 25$)

Табл. 2. Сводная таблица основных показателей надежности в зависимости от объема обучающей выборки $\kappa^{(C)}$ и от использования ПИ, при $I_{ПИ} = 5$, $Q = 4$

База	$\kappa^{(C)}$	$I_{ВИ}$	$N_{ВИ}$	$N_{ПИ}^{(max)}$	EER
Б1	25	1500	50	0	0,1167
Б1	25	1500	50	50	0,1028
Б1	40	1050	50	0	0,0821
Б1	40	1050	50	25	0,0798
Б2	27	1500	50	0	0,058
Б2	27	1500	50	25	0,0612
Б3	27	1500	50	0	0,0284
Б3	27	1500	50	25	0,0265

Чем дольше обучается ИИС, тем надежнее ее решения, но чем лучше обучена ИИС, тем больше времени требуется, чтобы поднять надежность еще выше (рис. 5*а*). Процесс обучения является достаточно устойчивым, но при высоких значениях $I_{ВИ}$ все-таки наблюдается незначительная склонность к переобучению. При увеличении $N_{ВИ}$ (рис. 5*б*) показатель EER монотонно снижается, темп снижения постепенно ослабляется и почти полностью останавливается, когда решения детекторов ВИ становятся сильно зависимыми (что неизбежно при росте их количества).

Оценка характера влияния других параметров на результаты работы ИИС является темой дальнейших исследований. На данном этапе можно утверждать, что разработанная модель и алгоритмы ее обучения удовлетворяют основным принципам построения ИИС [21], которые применительно к настоящей работе можно переформулировать так:

1. Распределенный характер вычислений и проявление эмерджентности (ИИС может повышать качество решений в процессе функционирования, в отличие от базовых классификаторов, точность распознавания для ИИС выше, чем для каждого классификатора в отдельности).
2. Достаточно устойчивый процесс обучения (склонность к переобучению незначительна при формировании ВИ).

3. Способность ИИС к адаптации, обусловленная двойной пластичностью: структурной и параметрической (меняются параметры и состав детекторов).
4. Взаимодействие – врожденный иммунитет формирует параметры, которые влияют на механизм подкрепления детекторов приобретенного иммунитета.
5. Надежность решений ИИС зависит от объема и чувствительности популяции детекторов.
6. Формирование памяти при помощи механизма приобретенного иммунитета.

Заключение

Предложены модель искусственной иммунной системы и алгоритмы ее обучения с учителем и с подкреплением. Предложенные решения основаны на применении методов математической статистики, ансамблей классификаторов, многомерных функционалов Байеса [1, 19], а также аналогий с теориями о естественной иммунной системе. В настоящей работе не приводится строгих доказательств сходимости предложенных алгоритмов, но даны достоверные свидетельства, доводы и результаты эмпирических исследований, которые говорят об их высокой эффективности. В задаче аутентификации по клавиатурному почерку разработанная ИИС превосходит многослойные ИНС (и другие рассмотренные в работах [8 – 12] методы) либо дает сопоставимые с ними показатели ошибок распознавания при гораздо меньшем объеме обучающей выборки (в разы). При этом ИИС легко обучить, достаточно лишь указать параметры $N_{ВИ}$ и $N_{ПИ}$, напрямую влияющие на объем ИИС и надежность ее решений, а также $I_{ВИ}$ и $I_{ПИ}$, напрямую влияющие на длительность обучения, время принятия решений и их надежность (обучение является устойчивым независимо от данных параметров).

Хочется подчеркнуть, что в настоящей работе не утверждается превосходство предложенного аппарата над нейронными сетями в общем случае. Это разные инструменты для решения разных задач. Их также можно использовать совместно. Например, извлечение признаков может выполняться при помощи глубокой сверточной нейронной сети (предварительно обученной «сжимать» образ до определенного количества признаков), а распознавание образов – с помощью иммунной модели.

Мощность предложенной модели ИИС связана с количеством вариаций мер близости, используемых в основе детекторов. В рамках будущих исследований целесообразно создать таблицу, в которой будут представлены различные функционалы, их параметры и свойства, чтобы сделать генерацию детекторов более эффективной под конкретную задачу.

Предложенный аппарат столкнулся со следующими проблемами:

– детекторы способны работать только с признаками, но не способны анализировать «сырые» данные. Требуется разработать архитектуру детекторов, способных извлекать признаки (по аналогии со сверточными сетями);

– разработанная модель не позволяет решать задачи кластеризации и регрессии. Требуется разработать адаптированную для данных задач модель ИИС;

– в разработанной модели имеется незначительная склонность к переобучению при формировании ВИ (исправить этот недостаток видится возможным, если контролировать коррелированность решений детекторов непосредственно либо изменять гиперпараметры ИИС в зависимости от ИНР). Устойчивость процесса дообучения при формировании ПИ пока мало изучена, что требует дальнейших исследований.

Тем не менее, данные проблемы не являются критическими и могут быть решены. Дальнейшие исследования планируется направить на поиск решений указанных проблем, а также: на оценку влияния параметров Q, $N_{ПИ}$, $I_{ПИ}$; разработку и обоснование механизма мутаций детекторов; применение разработанных положений в других задачах; оптимизацию кода и алгоритмов (с использованием параллельных вычислений) для ускорения обучения.

Благодарности

Работа выполнена при финансовой поддержке РФФИ (грант № 18-37-00399).

Литература

1. **Иванов, А.И.** Оценка надежности верификации автографа на основе искусственных нейронных сетей, сетей многомерных функционалов Байеса и сетей квадратичных форм / А.И. Иванов, П.С. Ложников, А.Е. Сулавко // Компьютерная оптика. – 2017. – Т. 41, № 5. – С. 765-774. – DOI: 10.18287/2412-6179-2017-41-5-765-774.
2. **Timmis, J.** Challenges for artificial immune systems / J. Timmis. – In: Neural Nets. WIRN 2005, NAIS 2005 / ed. by B. Apolloni, M. Marinaro, G. Nicosia, R. Tagliaferri. – Berlin, Heidelberg: Springer, 2005. – P. 335-367. – DOI: 10.1007/11731177_42.
3. **Mishra, P.K.** Artificial immune system: State of the art approach / P.K. Mishra, M. Bhusry // International Journal of Computer and Applications. – 2015. – Vol. 120, Issue 20. – P. 25-32. – DOI: 10.5120/21344-4357.
4. **Сулавко А.Е** Иммунные алгоритмы распознавания образов и их применение в биометрических системах (Обзор) / А.Е. Сулавко, Е.В. Шалина, Д.Г. Стадников, А.Г. Чобан // Вопросы защиты информации. – 2019. – № 1. – С. 38-46.
5. **Corus, D.** Fast artificial immune systems / D. Corus, P.S. Oliveto, D. Yazdani. – In: Parallel Problem Solving from Nature – PPSN XV. PPSN 2018 / ed. by A. Auger, C. Fonseca, N. Lourenço, P. Machado, L. Paquete, D. Whitley. – Cham: Springer, 2018. – P. 67-78. – DOI: 10.1007/978-3-319-99259-4_6.
6. **Zhang, C.** Ensemble machine learning. Methods and applications / C. Zhang, Y. Ma. – Boston, MA: Springer, 2012. – 329 p. – DOI: 10.1007/978-1-4419-9326-7.
7. **Сулавко, А.Е.** Влияние функционального состояния оператора на параметры его клавиатурного почерка в системах биометрической аутентификации / А.Е. Сулавко // Датчики и системы. – 2017. – № 11. – С. 19-30.

8. **Kobojek, P.** Application of recurrent neural networks for user verification based on keystroke dynamics / P. Kobojek, K. Saeed // Journal of Telecommunications and Information Technology. – 2016. – Vol. 3. – P. 80-90.
9. **Hellström, E.** Feature learning with deep neural networks for keystroke biometrics: A study of supervised pre-training and autoencoders. Computer Science and Engineering, master's level / E. Hellström. – Luleå: Luleå University of Technology, 2018. – 75 p.
10. **Killourhy, K.S.** Comparing anomaly detectors for keystroke dynamics / K.S. Killourhy, R.A. Maxion // Proceedings of the 39th Annual International Conference on Dependable Systems and Networks (DSN-2009). – 2009. –P. 125-134.
11. **Mulionoa, Y.** Keystroke dynamic classification using machine learning for password authorization / Y. Mulionoa, H. Hamb, D. Darmawan// Procedia Computer Science. – 2018. – Vol. 135. – P. 564-569.
12. **Antal, M.** Keystroke dynamics on Android platform / M. Antal, L.Z. Szabó, I. Laszlo // Proceedings of the 8th International Conference Interdisciplinarity in Engineering. – 2014. – P. 820-826.
13. **Сулавко, А.Е.** Высоконадежная двухфакторная биометрическая аутентификация по рукописным и голосовым паролям на основе гибких нейронных сетей / А.Е. Сулавко // Компьютерная оптика. – 2020. – Т. 44, № 1. – С. 82-91. – DOI: 10.18287/2412-6179-CO-567.
14. **Sulavko, A.E.** Subjects authentication based on secret biometric patterns using wavelet analysis and flexible neural networks / A.E. Sulavko, D.A. Volkov, S.S. Zhumazhanova, R.V. Borisov // XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE). – 2018. – P. 218-227. – DOI: 10.1109/APEIE.2018.8545676.
15. **Иванов, А.И.** Нейросетевое обобщение классических статистических критериев для обработки малых выборок биометрических данных / А.И. Иванов, Е.Н. Куприянов, С.В. Туреев // Надежность. – 2019. – Т. 19, № 2. – Р. 22-27. – DOI: 10.21683/1729-2646-2019-19-2-22-27.
16. **Сулавко, А.Е.** Тестирование нейронов для распознавания биометрических образов при различной информативности признаков / А.Е. Сулавко // Прикладная информатика. – 2018. – № 1. – С. 128-143.
17. **Protasov, V.** A method for evolutionary decision reconciliation, and expert theorems / V. Protasov, Z. Potapova, E. Melnikov // The Third International Conference on Intelligent Systems and Applications (INTELLI 2014). – 2014. – P. 43-47.
18. **Сулавко, А.Е.** Биометрическая аутентификация пользователей информационных систем по клавиатурному почерку на основе иммунных сетевых алгоритмов / А.Е. Сулавко, Е.В. Шалина // Прикладная информатика. – 2019. – № 3(81). – С. 39-53.
19. **Ivanov, A.I.** Reducing the size of a sample sufficient for learning due to the symmetrization of correlation relationships between biometric data / A.I. Ivanov, P.S. Lozhnikov, Y.I. Serikova // Cybernetics and Systems Analysis. – 2016. – Vol. 52, Issue 3 – P. 379-385. – DOI: 10.1007/s10559-016-9838-x.
20. **Schapire, R.E.** Boosting the margin: A new explanation for the effectiveness of voting methods / R.E. Schapire, Y. Freund, P. Bartlett, W.S. Lee // The Annals of Statistics. – 1998. – Vol. 26, Issue 5. – P. 1651-1686,
21. **Bersini, H.** The immune learning mechansims: Recruitment, reinforcement and their applications / H. Bersini, F. Varela. – In: Computing with biological metaphors / ed. by R. Patton. – Chapman and Hall, 1994. – ISBN: 978-0-412-54470-5.

Сведения об авторе

Сулавко Алексей Евгеньевич, 1986 года рождения, в 2009 году окончил Сибирскую государственную автомобильно-дорожную академию по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем», кандидат технических наук, доцент кафедры комплексной защиты информации Омского государственного технического университета. Область научных интересов: биометрия, распознавание образов, машинное обучение, искусственный интеллект, защита информации. E-mail: *sulavich@mail.ru* .

ГРНТИ: 28.23.25
Поступила в редакцию 12 мая 2020 г. Окончательный вариант – 7 августа 2020 г.

An abstract model of an artificial immune network based on a classifier committee for biometric pattern recognition by the example of keystroke dynamics

A.E. Sulavko[1]
[1]*Omsk State Technical University, Mira, h. 11 Omsk, Russian Federation, 644050*

Abstract

An abstract model of an artificial immune network (AIS) based on a classifier committee and robust learning algorithms (with and without a teacher) for classification problems, which are characterized by small volumes and low representativeness of training samples, are proposed. Evaluation of the effectiveness of the model and algorithms is carried out by the example of the authentication task using keyboard handwriting using 3 databases of biometric metrics. The AIS developed possesses emergence, memory, double plasticity, and stability of learning. Experiments have shown that AIS gives a smaller or comparable percentage of errors with a much smaller training sample than neural networks with certain architectures.

Keywords: biometric authentication, bagging, boosting, feature subspaces, machine learning on small samples, ensembles of models.

Citation: Sulavko AE. An abstract model of an artificial immune network based on a classifiers committee for biometric pattern recognition by the example of keystroke dynamics. Computer Optics 2020; 44(5): 830-842. DOI: 10.18287/2412-6179-CO-717.

Acknowledgements: The work was financially supported by the Russian Foundation for Basic Research under RFBR research project No. 18-37-00399.

References

[1] Ivanov AI, Lozhnikov PS, Sulavko AE. Evaluation of signature verification reliability based on artificial neural networks, Bayesian multivariate functional and quadratic forms, Computer Optics 2017; 41(5): 765-774. DOI: 10.18287/2412-6179-2017-41-5-765-774.

[2] Timmis J. Challenges for artificial immune systems. In Book: Neural Nets. WIRN 2005, NAIS 2005. Berlin, Heidelberg: Springer, 2005: 335-367. DOI: 10.1007/11731177_42.

[3] Mishra PK, Bhusry M. Artificial immune system: State of the art approach. Int J Comput Appl 2015; 120(20): 25-32. DOI: 10.5120/21344-4357.

[4] Sulavko AE, Shalina EV, Stadnikova DG, Choban AG. Immune algorithms for pattern recognition and their application in biometric systems (Review) [In Russian]. Information Security Issues 2019; 1: 38-46.

[5] Corus D, Oliveto PS, Yazdani D. Fast artificial immune systems. In Book: Auger A, Fonseca C, Lourenço N, Machado P, Paquete L, Whitley D, eds. Parallel Problem Solving from Nature – PPSN XV. PPSN 2018. Cham: Springer, 2018: 67-78. DOI: 10.1007/978-3-319-99259-4_6.

[6] Zhang C, Ma Y. Ensemble machine learning. Methods and applications, Boston, MA: Springer; 2012.

[7] Sulavko AE. Computer user's recognition based on keyboard handwriting dynamics with using of additional features from special sensors [In Russian]. Sensors and Systems 2017; 11: 19-30.

[8] Kobojek P, Saeed K. Application of recurrent neural networks for user verification based on keystroke dynamics. J Telecommun Inf Technol 2016; 3: 80-90.

[9] Hellström E. Feature learning with deep neural networks for keystroke biometrics: A study of supervised pre-training and autoencoders. Computer Science and Engineering, master's level. Luleå: Luleå University of Technology; 2018.

[10] Killourhy KS, Maxion RA. Comparing anomaly detectors for keystroke dynamics, Proc 39th Annual Int Conf on Dependable Systems and Networks 2009; 125-134.

[11] Mulionoa Y, Hamb H, Darmawan D. Keystroke dynamic classification using machine learning for password authorization. Procedia Comput Sci 2018; 135: 564-569.

[12] Antal M, Szabó LZ, Laszlo I. Keystroke dynamics on Android platform. Proc 8th Int Conf Interdisciplinarity in Engineering 2014; 820-826.

[13] Sulavko AE. Highly reliable two-factor biometric authentication based on handwritten and voice passwords using flexible neural networks. Computer Optics 2020; 44(1): 82-91. DOI: 10.18287/2412-6179-CO-567.

[14] Sulavko AE, Volkov DA, Zhumazhanova SS, Borisov RV. Subjects authentication based on secret biometric patterns using wavelet analysis and flexible neural networks. XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE) 2018; 218-227. DOI: 10.1109/APEIE.2018.8545676.

[15] Ivanov AI, Kuprianov EN, Tureev SV. Neural network integration of classical statistical tests for processing small samples of biometrics data [In Russian]. Dependability 2019; 19(2): 22-27. DOI: 10.21683/1729-2646-2019-19-2-22-27.

[16] Sulavko AE. Testing of neurons based on statistical functionals for verifying biometric images in feature space with different informativeness [In Russian]. Applied Informatics 2018; 1: 128-143.

[17] Protasov V, Potapova Z, Melnikov E. A method for evolutionary decision reconciliation, and expert theorems. 3rd Int Conf on Intelligent Systems and Applications (INTELLI 2014) 2014: 43-47.

[18] Sulavko AE, Shalina EV. Biometric authentication of users of information systems by keyboard handwriting based on immune network algorithms [In Russian]. Applied Informatics 2018; 3(81): 128-143.

[19] Ivanov AI, Lozhnikov PS, Serikova YI. Reducing the size of a sample sufficient for learning due to the symmetrization of correlation relationships between biometric data. Cybern Syst Anal 2016; 52(3): 379-385. DOI: 10.1007/s10559-016-9838-x.

[20] Schapire RE, Freund Y, Bartlett P, Lee WS. Boosting the margin: A new explanation for the effectiveness of voting methods. Ann Stat 1998; 26(5): 1651-1686.

[21] Bersini H, Varela F. The immune learning mechanisms: Recruitment reinforcement and their applications. In Book: Patton R, ed. Computing with biological metaphors. L.: Chapman and Hall, 1994. ISBN: 978-0-412-54470-5

Author's information

Alexey E. Sulavko (b. 1986) in 2009 graduated from Siberian State Automobile and Highway Academy with a degree in Integrated Information Security of Automated Systems. Candidate of Technical Sciences, Assistant Professor, Complex Information Protection department of Omsk State Technical University. Research interests are biometry, pattern recognition, machine learning, artificial intelligence, information security. E-mail: *sulavich@mail.ru* .

Received May 12, 2020. The final version – August 7, 2020.