ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

Х А Б А Р Ш Ы С Ы

ВЕСТНИК

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

THE BULLETIN

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

1944 ЖЫЛДАН ШЫҒА БАСТАҒАН
ИЗДАЕТСЯ С 1944 ГОДА
PUBLISHED SINCE 1944

6

АЛМАТЫ
АЛМАТЫ
ALMATY

2017

NOVEMBER
НОЯБРЬ
ҚАРАША

«Қазақстан Республикасы Ұлттық ғылым академиясының Хабаршысы».
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы»РҚБ (Алматы қ.)
Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде 01.06.2006 ж. берілген **№5551-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік

Мерзімділігі: жылына 6 рет.
Тиражы: 2000 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., 220, тел.: 272-13-19, 272-13-18,
www: nauka-nanrk.kz, bulletin-science.kz

Типографияның мекенжайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

«Вестник Национальной академии наук Республики Казахстан».
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№5551-Ж**, выданное 01.06.2006 г.

Периодичность: 6 раз в год
Тираж: 2000 экземпляров

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел. 272-13-19, 272-13-18.
www: nauka-nanrk.kz, bulletin-science.kz

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75

Bulletin of the National Academy of Sciences of the Republic of Kazakhstan.
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5551-Ж, issued 01.06.2006

Periodicity: 6 times a year
Circulation: 2000 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
http://nauka-nanrk.kz /, http://bulletin-science.kz

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 6, Number 370 (2017), 75 – 84

B. Ahmetov[1], N. Seilova[1], K. Boskebeev[2], Zh. Alimseitova[1]

[1]Kazakh National Technical Research University Named after K. I. Satpaev, Almaty, Kazakhstan,
[2]Kyrgyz State Technical University named after I. Razzakov, Bishkek, Kyrgyzstan

APPLICATION OF ARTIFICIAL NEURAL NETWORKS FOR BIOMETRIC IMAGES RECOGNITION

Abstract. The development of information technology leads to new requirements for the development of security systems, identity authentication and other protection mechanisms. The article is devoted to the use of artificial neural networks for biometric images recognition that are used in high-authentication systems. There is given a general structure of the biometric-neural network authentication system, the structural scheme of information processing in biometric-neural network authentication systems, the structural scheme for learning the neural network converter of the biometric parameters vectors in the key code (password). There is formed and trained a network of neurons, are formed neural network containers on the basis of structures. The choice of the length of the biocode of neural network converters is substantiated. After graduation, testing is conducted and the probabilities of errors of the first and second kind are determined.

Keywords: artificial neural networks, authentication, biometric image, neural network training, neural network containers, neural network testing, first-kind errors, second-kind errors.

УДК 004.056.53(045)

Б. Ахметов[1], Н. Сейлова[1], К. Боскебеев[2], Ж. Алимсеитова[1]

[1]Казахский национальный исследовательский технический университет им. К. И. Сатпаева, Алматы, Казахстан,
[2]Кыргызский государственный технический университет им. И. Раззакова, Бишкек, Кыргызстан

ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РАСПОЗНАВАНИЯ БИОМЕТРИЧЕСКИХ ОБРАЗОВ

Аннотация. Развитие информационных технологий ведет за собой новые требования к развитию систем обеспечения безопасности, аутентификации личности и других механизмов защиты. Статья посвящена применению искусственных нейронных сетей для распознавания биометрических образов, которые применяются в системах высоконаждежной аутентификации. Приведена общая структура системы биометрико-нейросетевой аутентификации, структурная схема обработки информации в системах биометрико-нейросетевой аутентификации, структурная схема обучения нейросетевого преобразователя векторов биометрических параметров в код ключа (пароля). На основе структур формируется и обучается сеть нейронов, формируются нейросетевые контейнеры. Обосновывается выбор длины биокода нейросетевых преобразователей. После окончания обучения проводится тестирование и определяются вероятности ошибок первого и второго рода.

Ключевые слова: искусственные нейронные сети, аутентификация, биометрический образ, обучение нейронной сети, нейросетевые контейнеры, тестирование нейронной сети, ошибки первого рода, ошибки второго рода.

Использование больших нейронных сетей. Использование больших нейронных сетей позволяет учитывать наряду с «хорошими» биометрическими данными «плохие» биометрические данные и «очень плохие» биометрические данные. При этом чем «хуже» используемые биометрические данные, тем больше должна быть сеть искусственных нейронов и тем сложнее ее обучать.

Общая структура системы биометрико-нейросетевой аутентификации показана на рисунке 1.

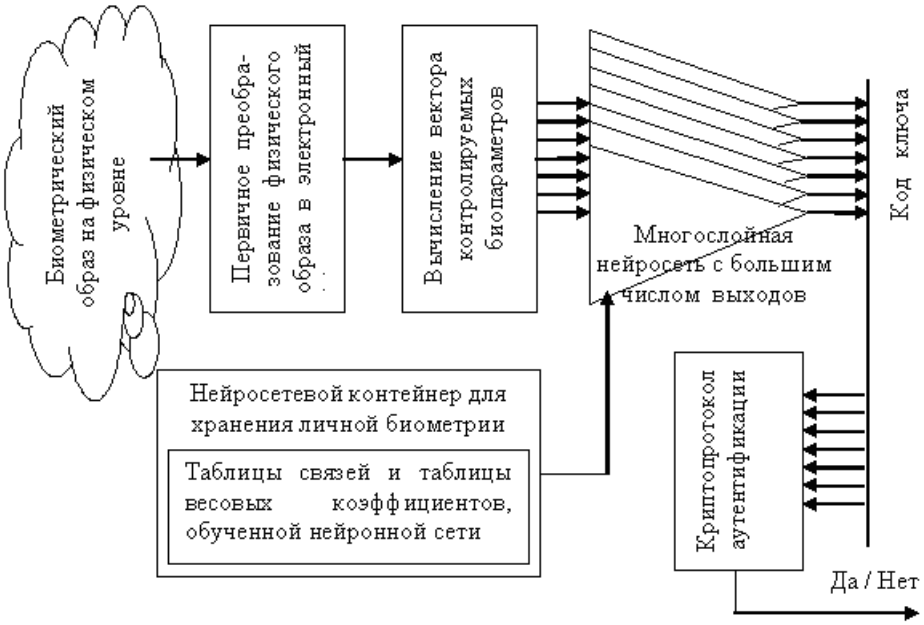

Рисунок 1 – Общая структура системы биометрико-нейросетевой аутентификации

При этом необходимо отметить, что для решения подобной задачи искусственные нейронные сети низкой размерности непригодны [2-4].

Процесс преобразования входного биометрического образа в выходной длинный пароль (ключ) можно представить в виде схемы на рисунке 2 [5].

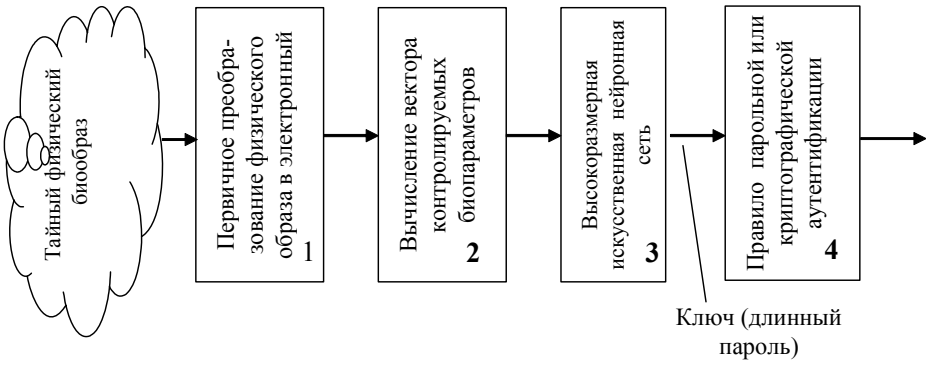

Рисунок 2 – Структурная схема обработки информации в системах биометрико-нейросетевой аутентификации

Общая схема обучения нейросетевых преобразователей биометрия – код. Схема обучения нейросетевого преобразователя векторов биометрических параметров в код ключа (пароля) представлена на рисунке 3 [1]. Для обучения необходимо N_1 примеров векторов "Свой" и N_2 примеров векторов "Чужие".

Обучение искусственной нейронной сети должно осуществляться автоматически (без вмешательства человека в процесс подбора параметров искусственной нейронной сети), пользователь должен иметь гарантии того, что его длинный пароль (ключ), участвующий в обучении, не будет скомпрометирован.

При обучении весовые коэффициенты искусственной нейронной сети должны подбираться автоматом обучения таким образом, чтобы при появлении на входах искусственной нейронной сети элементов вектора «Свой» на выходах искусственной нейронной сети появлялся длинный

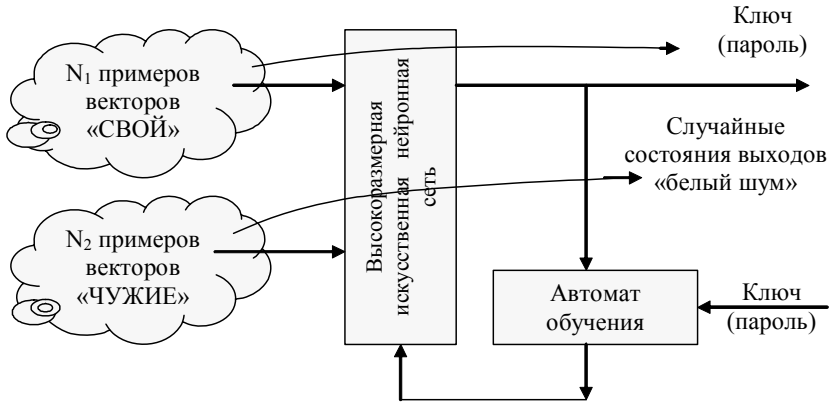

Рисунок 3 – Структурная схема обучения нейросетевого преобразователя векторов биометрических параметров в код ключа (пароля)

пароль (ключ). При появлении на входах искусственной нейронной сети векторов данных, соответствующих образам «Чужой», на выходах искусственной нейронной сети должны появляться случайные состояния – «белый шум». Обучение осуществляется путем поочередного предъявления образов «Свой» и «Чужие» с промежуточным подбором коэффициентов.

Для того, чтобы воспользоваться нейросетевым обогащением био-данных, необходимо уметь обучать одиночные искусственные нейроны [6-10].

Формирование и обучение сети нейронов. Нейросетевые контейнеры. Для того, чтобы получить биокод ключа доступа, необходимо создать сеть нейронов с числом выходов, равным длине ключа. Чем больше входов у нейронной сети и чем больше выходов у нейронной сети, тем выше качество принимаемых решений. Насколько сильна подобная связь видно из данных таблицы.

Рост качества решений в зависимости от числа входов и выходов искусственной нейронной сети

Число входов нейросети	Число выходов нейросети	Вероятность отказа «Своему»	Вероятность пропуска «Чужого»
5 входов	1 выход, 2 класса	$P_1 = 0,1$	$P_2 = 0,17$
48 входов	1 выход, 2 класса	$P_1 = 0,1$	$P_2 = 0,03$
480 входов	1 выход, 2 класса	$P_1 = 0,1$	$P_2 = 0,005$
480 входов	256 выходов, 2^{256} классов	$P_1 = 0,1$	$P_2 = 0,000000001$
Обучение нейросети с 480 входами и 256 выходами велось на 20 примерах образа «Свой» и 128 примеров образов «Чужой» алгоритмом ГОСТ Р 52633.5–2011.			

Из таблицы видно, что простое увеличение числа входов числа учитываемых биометрических параметров не очень эффективно. Гораздо важнее чтобы параллельно с числом входов нейронной сети увеличивать число ее выходов. При одинаковом числе входов (480 входов) увеличение числа выходов с 1 до 256 дает выигрыш в качестве принимаемых нейронной сетью решения примерно в миллиард раз. При этом время и иные затраты вычислительных ресурсов увеличиваются примерно в 100 раз, видна экспоненциальная связь размеров искусственного интеллекта и качества принимаемых им решений.

Одним из важнейших вопросов является выбор структуры, используемой нейронной сетью. Обычно в литературе по искусственным нейронным сетям разделяют сети на одно-, двух- и трехслойные, а также сети с большим, чем три, числом нейронов. Столь широкое многообразие структур нейронных сетей для биометрии не актуально. ГОСТ Р 52633.5–2011 предусматривает либо однослойные, либо двухслойные нейронные сети. Для двухслойных нейронных сетей функции

первого и второго слоев разделены. Нейроны первого слоя выполняют функцию обогащения биометрических данных и квантования обогащенных данных. Если качество обогащения оказалось недостаточно велико, то второй слой нейронов правит ошибки биокода нейронов первого слоя.

Следует отметить, что второй слой нейронов всегда может быть заменен обычным классическим кодом, обнаруживающим и исправляющим ошибки, однако нейросетевое корректирование ошибок выгоднее. Причина выгоды от применения нейросетевых корректоров состоит в том, что при обучении второго слоя на примерах биокодов «Свой» оценивают реальный показатель стабильности каждого из разрядов биокода.

Практика показывает, что подавляющее большинство разрядов биокода имеет высокую стабильность, нестабильными оказываются только отдельные разряды кода с точно известным положением.

Второй слой нейронов обучается корректировать нестабильные разряды и одновременно хэшировать (перемешивать) как стабильные, так и нестабильные разряды. Все классические коды с обнаружением и исправлением ошибок наоборот строятся в рамках гипотезы о равновероятном распределении ошибок между разрядами кода. Именно из-за этого классические самокорректирующиеся коды проигрывают нейросетевым корректорам ошибок, которые во время обучения учитывают реальное распределение показателей стабильности биокодов «Свой».

Кроме числа слоев нейронов сети необходимо выбирать число входов каждого нейрона и задать связи входов с номерами входов сети. Так, если вся нейросеть имеет 480 входов и средняя информативность входов составляет порядка 0,3 бита, то потребуется использовать нейроны с числом входов от 1 до 18 (в зависимости от качества используемых нейроном биометрических параметров и корреляционных связей между ними). Необходимое число входов может быть найдено только во время обучения нейрона. То есть изначально задают случайным выбором малое число входов далее, если качество решения не дотягивает до заданного, то увеличивают число входов нейрона. В конечном итоге получается однослойная сеть нейронов, причем каждый нейрон будет иметь свое число входов, подключенных случайно к входам всей сети. После обучения дополнительно получается таблица весовых коэффициентов для входных связей каждого из нейронов.

Формально обученная сеть описывается таблицами связей нейронов и таблицами весовых коэффициентов. Если сеть двухслойная, то таблицы номеров связей и таблицы весовых коэффициентов должны быть созданы для каждого из слоев нейронов. Слои нейронов обучаются последовательно. После обучения первого слоя нейронов проводят транслирование примеров образов «Свой» и «Все Чужие» с входа нейронной сети на выходы нейронов, получают примеры биокодов и обучают на них нейроны второго слоя.

Таблицы связей нейронной сети и таблицы весовых коэффициентов, обученных нейронов, образуют так называемые нейросетевые контейнеры. В нейросетевом контейнере информации достаточно, чтобы в нужный момент воспроизвести программно обученную нейросеть и преобразовать биометрические данные человека в код его криптографического ключа доступа. Процедура аутентификации, построенная с использованием нейросетевого контейнера, приведена на рисунке 4.

Формирование и использование нейросетевых контейнеров для хранения биометрии человека и интерфейсы взаимодействия с ними регламентируются ГОСТ Р 52633.4–2012 [10].

Фактически обучение искусственных нейронных сетей по ГОСТ Р 52633.5–2011 при увеличении числа входов у нейронов осуществляется все устойчивее и устойчивее. Именно по этой причине большие нейронные сети после их обучения работают надежнее классических алгоритмов многомерной статистики и линейной алгебры. Построить квадратичное решающее правило в виде 480-мерного гиперэллипса технически невозможно, тогда как построить аппроксимацию этого гиперэлли пса 480-мерными параллелепипедами (4 персептрона с 480 входами в первом слое сети) вполне возможно.

Рациональный выбор длины биокода нейросетевых преобразователей. Если нам требуется для последующей криптографической аутентификации длина ключа 256 бит, то из этого условия однозначно вытекает, что нейросетевой преобразователь биометрия-код должен иметь 256 выходов. Если нейросетевой преобразователь однослойный, то уже первый слой должен иметь 256 нейронов.

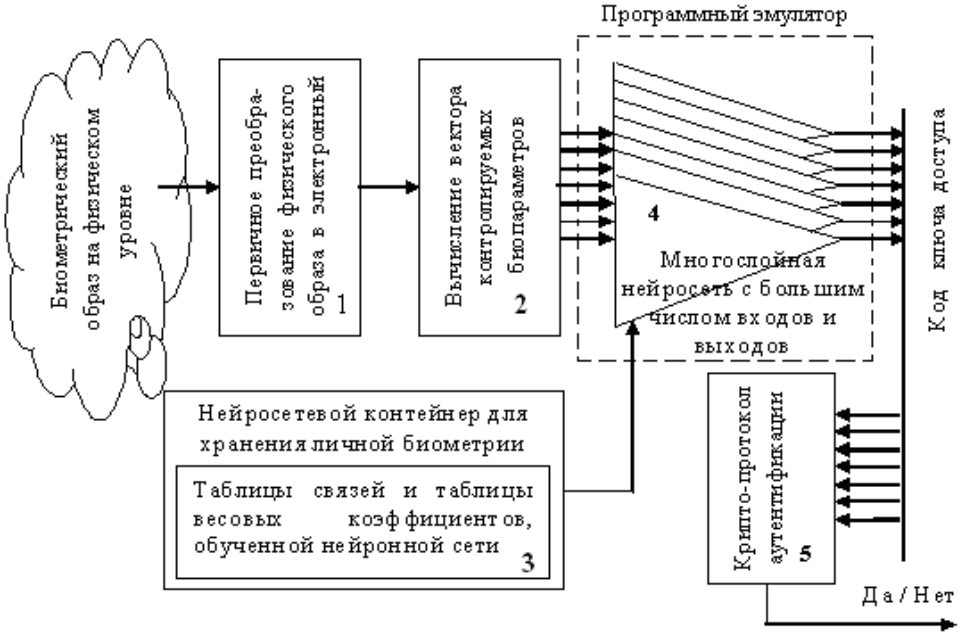

Рисунок 4 – Блок-схема биометрической аутентификации с использованием нейросетевого контейнера

Криптографическая защита всегда намного сильнее парольной защиты и биометрической защиты. Этот факт хорошо наблюдаем, когда изменяем число нейронов в первом слое сети. В первом приближении вероятность биометрических ошибок $P_{2,Б}$ будет уменьшаться с ростом числа использованных нейронов, соответствующие кривые снижения отображены на рисунке 5. Однако быстрый рост стойкости (быстрое снижение вероятности $P_{2,Б}$) происходит не постоянно. Обычно линейное снижение вероятности $P_{2,Б}$ наблюдается только на начальном участке роста числа нейронов. Далее происходит замедление роста показателя и, начиная с некоторого момента, вероятность ошибок второго рода вообще перестает снижаться.

Момент, когда происходит остановка снижения вероятности ошибок второго рода, зависит от информативности биометрического образа «Свой». На рисунке 5 представлены две кривые снижения вероятности ошибок биометрической составляющей аутентификации.

Из рисунка 5 видно, что «слабый» мало информативный биометрический образ дает большее значение вероятности ошибок ($P_{2,Б} = 10^{-4,7}$), насыщение для этого образа возникает при длине ключа 128 бит, то есть при длине выходного кода 256 бит имеем 50%-ю избыточность кода, которая безболезненно может расходоваться на обнаружение и исправление ошибок.

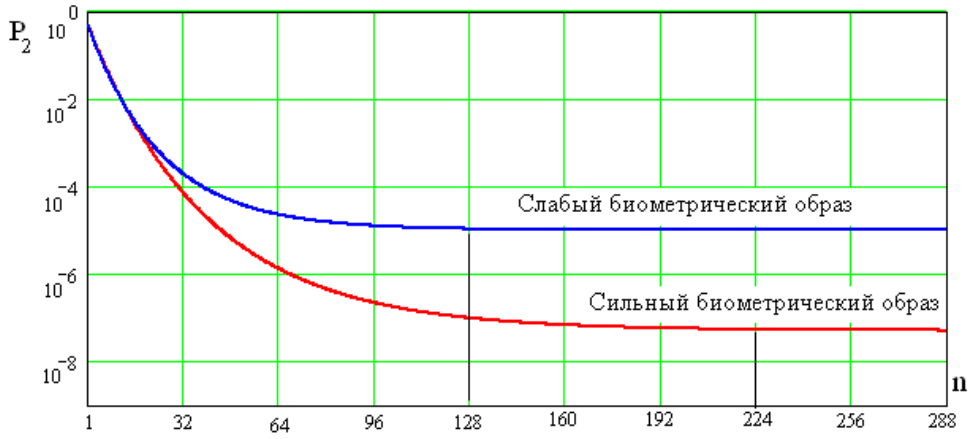

Рисунок 5 – Влияние числа выходов однослойной нейронной сети на значение вероятности ошибок второго рода

Более «сильный» биометрический образ имеет участок насыщения для кодов длиной более 224 разряда ($P_{2,Б} = 10^{-7,1}$), то есть для этого кода избыточность составит 12,5%. Эта избыточность также может быть использована для обнаружения и исправления ошибок классическими самокорректирующимися кодами. Если этой избыточности не хватает, то следует увеличить длину выходного биокода до необходимой.

В некоторых случаях (например, при использовании зарубежных криптографических алгоритмов) длина ключа может оказаться меньше длины до начала участка насыщения биометрико-нейросетевой защиты. Эта ситуация как раз соответствует второму случаю применения относительно «сильной» биометрии (нижняя кривая рисунка 5) при необходимой длине ключа 128 бит. Формально можем ограничиться 128 нейронами в первом слоне нейронной сети, однако это приведет к определенным потерям показателей качества.

В случаях, когда технически выгодно иметь число нейронов больше длины выходного криптографического ключа (например, 224 > 128), необходимо осуществить хэширование биокода. После хэширования следует обрезать хэш-функцию до нужной длины и использовать ее в качестве ключа.

В том случае, когда ключи изготавливаются вне биометрического приложения, привести значение хэш-функции к заданному значению удается, если сложить ее по модулю два с дополнением.

Заметим, что описанный выше прием годится не только для сокращения длины ключа, но и для увеличения его длины. Это означает, что для относительно «слабого» биометрического образа «Свой» (верхняя кривая рисунка 5) можно обойтись сетью со 128 искусственными нейронами, увеличив далее длину биокода хэшированием со 128 до 256 бит. Подобный прием целесообразен для экономии вычислительных ресурсов. Криптографическое хэширование обычно выполняется примерно в 1000 раз быстрее, чем программное эмулирование искусственной нейронной сети.

Нейросетевая коррекция биокода вторым слоем нейронов. В том случае, если классические самокорректирующиеся коды дают слишком большие информационные потери (требуют слишком большой избыточности), ГОСТ Р 52633.5–2011 рекомендует использовать нейроны второго слоя для коррекции ошибок, допущенных нейронами первого слоя. Перед настройкой нейронов второго слоя стандарт рекомендует оценить стабильность каждого из разрядов биокода «Свой». Для этой цели подают тестовые примеры образа «Свой» и вычисляют вероятности ошибок первого рода по каждому из разрядов $P_{1,i}$. Далее вычисляют показатели стабильности каждого из разрядов:

$$\gamma_i = 2 \cdot \left| P_{1,i} - 0.5 \right|, \qquad (1)$$

где γ_i – показатель стабильности i-го разряда, принимающий значения 1.0 для абсолютно стабильных разрядов и значение 0.0 – для нестабильных разрядов с равновероятными состояниями «0» и «1».

При настройке нейрона второго слоя необходимо задавать его весовые коэффициенты пропорционально показателю стабильности (1). Знак весового коэффициента выбирается случайно. Входы корректирующего нейрона подключают к разрядам биокода случайно, при этом осуществляют преобразование значений разрядов биокода: состояние «0» преобразуют в состояние –1, состоянию «1» присваивается значение +1. В результате перемножения случайных знаков весовых коэффициентов и случайных состояний разрядов биокода ±1 на выходе сумматора нейрона появляется состояние, близкое к нулю.

Настройка нейрона сводится к случайным циклическим перестановкам знака у пар входов. Очевидно, что у нейрона с 64 входами максимально возможное выходное состояние составит близкое к величине +64, а минимально возможное значение будет близко к –64. Если настраиваемый нейрон должен править 1 ошибку и давать состояние «1», то необходимо добиться максимального значения отклика на примеры «Свой», близкого к +2. Если настраиваемый нейрон должен править 1 ошибку и давать состояние «0», то необходимо добиться максимального значения отклика на примеры «Свой», близкого к –2. Число ошибок, исправляемых нейроном, должно быть всегда примерно на единицу меньше модуля максимального отклика на примеры «Свой».

Следует отметить, что второй слой нейронов выполняет две функции. Во-первых, он правит ошибки биокода предыдущего слоя нейронов, во-вторых, сумматоры второго слоя нейронов (перемешивают) хэшируют данные кодов «Чужой».

Хэширование данных «Чужой», выполняемое нейронами второго слоя. Идеальный преобразователь биометрия-код должен полностью исключать неопределенность кодов «Свой» и максимально усиливать энтропию кодов «Чужой». Входные энтропии непрерывных данных примеров образа «Свой» и примеров образа «Чужой» сопоставимы:

$$H_{480}(\bar{v}) \approx \mathrm{H}_{480}(\bar{\xi}). \tag{2}$$

где $H_{480}(\bar{v})$ – входная энтропия непрерывных данных примеров образа «Свой»; $\mathrm{H}_{480}(\bar{\xi})$ – входная энтропия непрерывных данных примеров образа «Чужой».

После осуществления нейросетевого преобразования ситуация меняется:

$$\begin{cases} H_{256}(c) \approx 0; \\ H_{256}(x) \approx 256. \end{cases} \tag{3}$$

По сути дела, то, на сколько мала энтропия кодов «Свой» и на сколько близка энтропия кодов «Чужой» к предельному значению 256 бит, определяет близость реального преобразователя к идеальному.

Двухслойная нейросеть улучшает свои свойства от слоя к слою, то есть, обозначив коды первого слоя индексом 1, а коды второго – индексом 2, можно записать

$$\begin{cases} H_{256}(c_1) \rangle H_{256}(c_2) \approx 0; \\ H_{256}(x_1) \langle H_{256}(x_2) \approx 256. \end{cases} \tag{4}$$

Эта ситуация видна на соответствующих распределениях расстояний Хэмминга кодов «Свой» и кодов «Чужой» (рисунок 6).

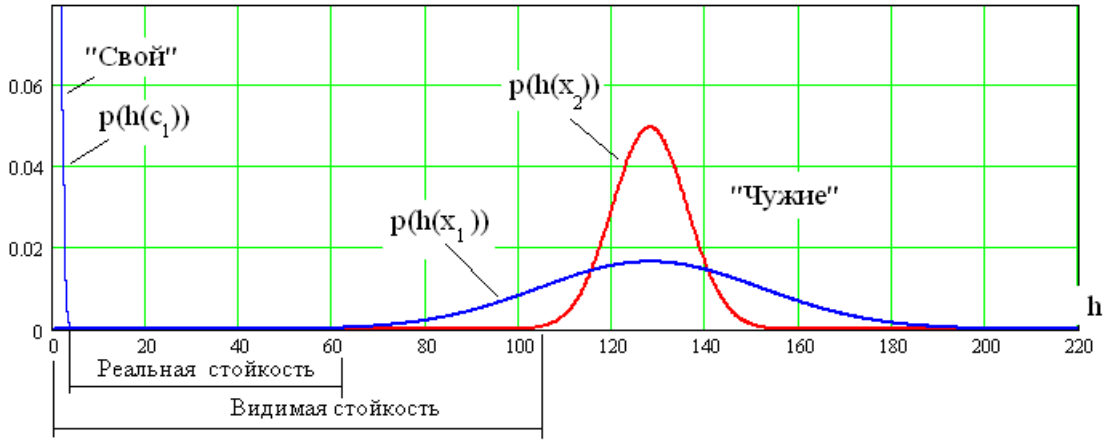

Рисунок 6 – Сжатие распределения расстояний Хэмминга
на выходе нейронов второго слоя из-за хэширующих свойств нейронов

Из рисунка 6 видно, что на выходе нейронов первого слоя биокод имеет стойкость к атакам подбора примерно 56 бит (расстояние между краями распределений расстояний Хэмминга «Свой» и «Чужие»). После корректировки ошибок нейронами второго слоя видимое расстояние между множествами составляет более чем 100 бит, однако это мнимая (завышенная) стойкость, обусловленная тем, что нейроны второго слоя не только правят биокод «Свой», но и хэшируют коды «Чужой». Хэширующие свойства второго слоя нейронов можно оценить как отношение энтропии кодов «Чужой» на выходе нейросети к энтропии биокодов на выходе нейронов первого слоя.

То, что нейроны второго слоя сети обладают достаточно сильными хэширующими свойствами, объясняется случайной расстановкой знаков весовых коэффициентов и выполняемой ими

операцией округления результатов суммирования. Любая однонаправленная операция, приводящая к уменьшению длины кода, обладает некоторыми хэширующими свойствами, так как по коротким выходным кодам нельзя восстановить исходные данные. В нашем случае результаты суммирования исправляющего код нейрона могут меняться в интервале от –64 до +64, а его выходной код имеет только два значения «0» и «1». Присутствует операция усечения длины 9-разрядного кода до 1-го разряда.

Вероятности ошибок первого и второго рода. После обучения системы биометрико-нейросетевой аутентификации необходимо оценить качество обучения. Оцениваются вероятность ошибки первого рода P_1 и вероятность ошибки второго рода P_2.

Пользователь должен знать реальные оценки стойкости к атакам подбора конкретной реализации биометрической аутентификации после ее обучения, построенной на воспроизведении конкретного тайного биометрического образа. Тестирование осуществляют, используя N_1 – тестовых примера векторов образов «Свой» и N_2-тестовых примера векторов образов «Чужой». Структурная схема тестирования приведена на рисунке 7.

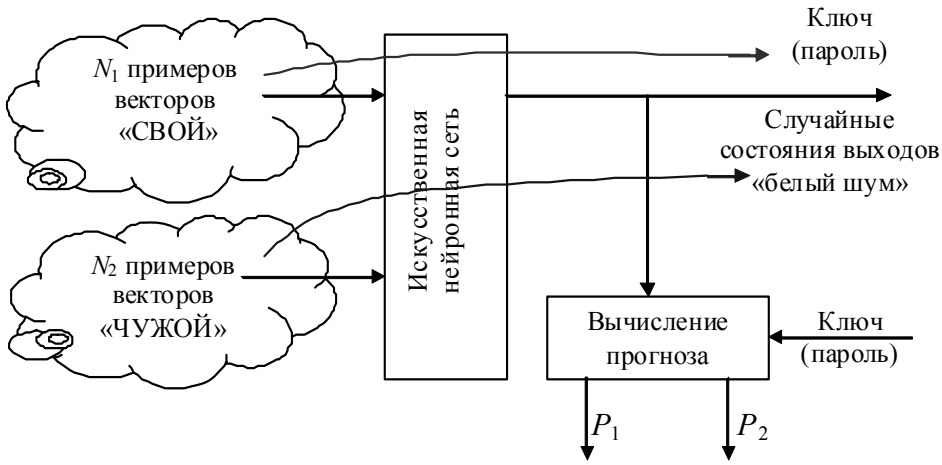

Рисунок 7 – Структурная схема тестирования системы биометрико-нейросетевой аутентификации после обучения

Всякая биометрическая защита строится на том, что она способна хорошо распознавать образ «Свой» и надежно выделять множество образов «Чужие» («Все Чужие»). Очевидно, что средство биометрической защиты (биометрической аутентификации) может ошибаться. Основной задачей (задачей № 1) для биометрии является обеспечение доступа донору биометрического образа «Свой». Ошибка при выполнении этой задачи рассматривается как ошибка первого рода. Основной характеристикой эффективности работы средства биометрической аутентификации является вероятность появления ошибок первого рода P_1.

Второй задачей средства биометрической аутентификации является препятствовать доступу донору образа «Чужой». Второй важнейшей характеристикой биометрических средств является вероятность появления ошибок второго рода P_2 из-за возможных коллизий образов «Свой» и «Чужой» на рассматриваемом множестве признаков (биометрических параметров).

Очевидно, что вероятность ошибок второго рода P_2 будет тем меньше, чем больше биометрических параметров принимает в расчет то или иное средство биометрической аутентификации. Высоконадежными можно считать только те биометрические средства, которые анализируют сотни или даже тысячи биометрических параметров. При этом атакующий не должен знать подбираемого биометрического образа, только в этом случае биометрия может рассматриваться как высоконадежная.

Выводы. Двухслойная сеть нейронов универсальна в совокупности со следующим за ней цифровым автоматом криптографической аутентификации. Эта совокупность позволяет создавать любые приложения биометрической защиты информации. Увеличение числа нейронов в слоях сети (в первом и во втором) является весьма и весьма эффективным техническим приемом.

На сегодняшний день лучшие средства высоконадежной биометрической аутентификации обеспечивают вероятность ошибок второго рода на уровне одной миллиардной и меньше, то есть

злоумышленник, пытающийся преодолеть биометрическую защиту, должен предъявить миллиард разных биометрических образов (например, воспроизвести своей рукой миллиард рукописных паролей). Если на воспроизведение одного рукописного пароля уходит 10 секунд, то злоумышленнику потребуется 10 миллиард секунд, что составит 321 год непрерывных усилий.

ЛИТЕРАТУРА

[1] Малыгин А.Ю., Ахметов Б.С. и др. Учет влияния корреляционных связей на результаты тестирования преобразователей биометрия-код // Информационные и телекоммуникационные технологии: образование, наука, практика: Сб. тр. межд.. науч.-практ. конф. – Алматы: КазНТУ, 2012. – С. 34-37.

[2] Болл Руд и др. Руководство по биометрии / Болл Руд, Коннел Джонатан Х. и др. – М.: Техносфера, 2007. – 368 с.

[3] Arakala A., Jeffers J., Horadam K. J. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication // Advances in Biometrics (LNCS 4642). Springer. – 2007. – P. 760-769.

[4] ГОСТ Р ИСО/МЭК 19784–1–2007 «Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс». – Ч. 1: Спецификация биометрического программного интерфейса. – М.: Стандартинформ, 2007.

[5] ГОСТ Р ИСО/МЭК 19784–2–2010 «Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс». – Ч. 2: Интерфейс поставщика биометрической функции архива. – М.: Стандартинформ, 2011.

[6] Круглов В.В., Дли М.И., Голунов Р.Ю. Нечёткая логика и искусственные нейронные сети. – М.: Физматлит, 2001. – 221 с.

[7] Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы / Пер. с польского И. Д. Рудинского. – М.: Горячая линия – Телеком, 2004.

[8] Саймон Хайкин. Нейронные сети: Полный курс. – М.: Вильямс, 2006. – С. 1104.

[9] Уоссермен Ф. Нейрокомпьютерная техника: теория и практика. – М.: Мир, 1992. – 240 с.

[10] Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Изд-во ПГУ, 2000.

REFERENCES

[1] Malygin A.Ju., Ahmetov B.S. i dr. Uchet vlijanija korreljacionnyh svjazej na rezul'taty testirovanija preobrazovatelej biometrija-kod // Informacionnye i telekommunikacionnye tehnologii: obrazovanie, nauka, praktika: Sb. tr. mezhd.. nauch.-prakt. konf. Almaty: KazNTU, 2012. P. 34-37.

[2] Boll Rud i dr. Rukovodstvo po biometrii / Boll Rud, Konnel Dzhonatan H. i dr. M.: Tehnosfera, 2007. 368 p.

[3] Arakala A., Jeffers J., Horadam K. J. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication // Advances in Biometrics (LNCS 4642). Springer. 2007. P. 760-769.

[4] GOST R ISO/MJeK 19784–1–2007 «Avtomaticheskaja identifikacija. Identifikacija biometricheskaja. Biometricheskij programmnyj interfejs». Part 1: Specifikacija biometricheskogo programmnogo interfejsa. M.: Standartinform, 2007.

[5] GOST R ISO/MJeK 19784–2–2010 «Avtomaticheskaja identifikacija. Identifikacija biometricheskaja. Biometricheskij programmnyj interfejs». Part 2: Interfejs postavshhika biometricheskoj funkcii arhiva. M.: Standartinform, 2011.

[6] Kruglov V.V., Dli M.I., Golunov R.Ju. Nechjotkaja logika i iskusstvennye nejronnye seti. M.: Fizmatlit, 2001. 221 p.

[7] Rutkovskaja D., Pilin'skij M., Rutkovskij L. Nejronnye seti, geneticheskie algoritmy i nechetkie sistemy / Per. s pol'skogo I. D. Rudinskogo. M.: Gorjachaja linija – Telekom, 2004.

[8] Sajmon Hajkin. Nejronnye seti: Polnyj kurs. M.: Vil'jams, 2006. P. 1104.

[9] Uossermen F. Nejrokomp'juternaja tehnika: teorija i praktika. M.: Mir, 1992. 240 p.

[10] Ivanov A.I. Biometricheskaja identifikacija lichnosti po dinamike podsoznatel'nyh dvizhenij. Penza: Izd-vo PGU, 2000.

Б. Ахметов[1], Н. Сейлова[1], К. Боскебеев[2], Ж. Алимсеитова[1]

[1]Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы, Қазақстан,
[2]И. Раззаков атындағы Қыргыз мемлекеттік техникалық университет, Бишкек, Қырғызстан

БИОМЕТРИЯЛЫҚ БЕЙНЕЛЕРДІ ТАНЫП БІЛУ ҮШІН ЖАСАНДЫ НЕЙРОНДЫ ЖЕЛІЛЕРДІ ҚОЛДАНУ

Аннотация. Ақпараттық технологиялардың дамуы өзінің артынан ақпараттық қауіпсіздікті қамтамасыз ету жүйелерінің, тұлғаның аутентификациясының және басқа қорғау тетіктерінің дамуына алып келді. Мақала жоғары сенімді аутентификация жүйелерінде қолданатын жасанды нейронды желілерді биометриялық бейнелерді танып білуге арналған. Биометриялық-нейрожелілік аутентификацияның жалпы құрылымы, биометриялық-нейрожелілік аутентификация жүйелерінде ақпаратты өңдеудің құрылымдық сұлбасы, биометриялық параметрлердің векторларын кілт (құпиясөз) кодына нейрожелілік түрлендіргішті оқытудың құры-

лымдық сұлбасы келтірілген. Құрылымдар негізінде нейрондар желісі қалыптастырылады және оқытылады, нейрожелілік контейнерлер қалыптастырылады. Нейрожелілік түрлендіргіштердің биокод ұзындығын таңдау негізделді. Оқытудан кейін тестілеу жүргізіледі және бірінші және екінші түр қателердің ықтималдықтары анықталады.

Түйін сөздер: жасанды нейронды желілер, аутентификация, биометриялық бейне, нейронды желіні оқыту, нейрожелілік контейнерлер, нейронды желіні тестілеу, бірінші түр қателері, екінші түр қателері.

Сведения об авторах:

Ахметов Бахытжан Сражатдинович – д.т.н., профессор кафедры Информационной безопасности Казахского национального исследовательского технического университете им. К. И. Сатпаева, bakhytzhan.akhmetov.54@mail.ru

Сейлова Нургуль Абадуллаевна – к. т. н., заведующий кафедрой Информационной безопасности Казахского национального исследовательского технического университете им. К. И. Сатпаева, seilova_na@mail.ru

Боскебеев Калычбек Джетмишбаевич – к.т.н., доцент Кыргызского государственного технического университета им. И. Раззакова, kboskebeev@mail.ru

Алимсеитова Жулдыз Кенесхановна – лектор кафедры Информационной безопасности Казахского национального исследовательского технического университете им. К. И. Сатпаева, zhuldyz_al@mail.ru

Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

ISSN 2518-1467 (Online), ISSN 1991-3494 (Print)

http://www.bulletin-science.kz/index.php/ru/

Редакторы *М. С. Ахметова, Т. М. Апендиев*
Верстка на компьютере *Д. Н. Калкабековой*

Подписано в печать 20.11.2017.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
14,4 п.л. Тираж 2000. Заказ 6.