КЫРГЫЗСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ И.АРАБАЕВА
КЫРГЫЗСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ И.РАЗЗАКОВА

Диссертационный Совет Д 05.18.584

На правах рукописи
УДК 007+681.322+681.5.015.42

АЛИМСЕИТОВА ЖУЛДЫЗ КЕНЕСХАНОВНА

Разработка интеллектуальной автоматизированной системы распознавания биометрических образов

05.13.16 - Применение вычислительной техники, математического моделирования и математических методов в научных исследованиях

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Бишкек - 2019

Работа выполнена в Кыргызском государственном техническом университете имени И. Раззакова

Научный руководитель: кандидат технических наук,
доцент Боскебеев К.Дж.

Официальные оппоненты: кандидат физико-математических наук,
доцент Султанов Р.К.

доктор физико-математических наук,
профессор Бийбосунов Б.И.

Ведущая организация: Университет «Туран»
050013, Республика Казахстан, г. Алматы,
ул. Сатпаева 16-18, 18а

Защита состоится “27” мая 2019 года в 16-00 часов на заседании Диссертационного совета Д.05.18.584 при Кыргызском государственном университете имени И. Арабаева и Кыргызском государственном техническом университета имени И. Раззакова по адресу: 720026, г. Бишкек, ул. Раззакова, 51, корпус №1, зал зас. 213, веб-сайт: www.arabaev.kg.

С диссертацией можно ознакомиться в библиотеках Кыргызского государственного университета имени И. Арабаева и Кыргызского государственного технического университета имени И. Раззакова по адресу: 720026, г. Бишкек, ул. Раззакова, 51 и
720044, г. Бишкек, пр. Ч. Айтматова 66

Автореферат разослан «26» апреля 2019 г.

Ученый секретарь
диссертационного совета
кандидат технических наук, доцент Исраилова Н.А.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации. В настоящее время для усиления защиты информационных ресурсов разрабатываются технологии биометрической аутентификации личности, где биометрические данные человека преобразуются в криптографический ключ или пароль. Для их реализации применяются интеллектуальные методы и модели, базирующиеся на теории нейронных сетей (НС).

Вопросы обеспечения безопасности, в том числе аутентификации пользователей при обработке информации, были обозначены в Государственной программе «Цифровой Казахстан» и нашли отражение в Концепции кибербезопасности «Киберщит Казахстана». Разработка указанной концепции и анализ научно-практических исследований в данной области показывают, что мало исследованными остаются вопросы повышения эффективности распознавания биометрических образов в информационных системах, что и обуславливает актуальность настоящего исследования.

Связь темы диссертации с крупными научными программами, основными научно-исследовательскими работами, проводимыми научными учреждениями. Диссертационная работа проводилась в рамках научно-исследовательских проектов КазНИТУ имени К.И. Сатпаева №753МОН.ГФ.13.13 «Исследование вариантов реализации и разработка действующего лабораторного образца ON-LINE системы биометрического обезличивания электронных историй болезней для медицинского учреждения», № 757.МОН.ГФ.15.ИИТ.6 «Исследование, гармонизация, модификация и постановка на учет группы стандартов по биометрической поддержке информационной безопасности», в рамках научно-исследовательского проекта КГТУ им. И. Раззакова «Моделирование и анализ безопасности граждан по базе данных биометрики Кыргызской Республики».

Цель и задачи исследования. Целью работы является повышение эффективности распознавания биометрических образов за счет применения биометрико-нейросетевых методов.

Задачами исследования являются:

– разработка нейросетевой модели, позволяющей эффективно распознавать пользователей на основе анализа геометрических параметров фрагментов рукописного текста изменяемого размера;

– снижение размерности входной выборки за счет учета корреляционных связей между выходными сигналами НС;

– разработка метода синтеза критерия хи-квадрат распределений зависимых данных;

– разработка автоматизированной интеллектуальной системы распознавания биометрических образов в информационных системах;

– разработка методики формирования биометрических баз рукописных образов и отпечатков пальцев;

– экспериментальное исследование автоматизированной интеллектуальной системы распознавания биометрических образов в информационных системах.

Научная новизна полученных результатов заключается в следующем:

– разработана композитная нейросетевая модель, которая за счет использования в сверточной НС модулей долгой краткосрочной памяти, а также за счет адаптации параметров модели к условиям системы биометрической аутентификации, обеспечивает эффективное распознавание пользователей на основе анализа геометрических параметров фрагментов рукописного текста изменяемого размера;

– предложен метод снижения входной выборки НС за счет учета корреляционных связей между выходными сигналами НС;

– предложен метод синтеза критерия хи-квадрат распределений зависимых данных, позволяющий существенно увеличить достоверность оценок проверки статистических гипотез;

– разработана архитектура автоматизированной интеллектуальной системы распознавания биометрических образов с использованием нейросетевых технологий;

– разработана методика формирования баз рукописных образов и отпечатков пальцев.

Практическая значимость полученных результатов. Предложенные нейросетевые модели и методы позволили разработать интеллектуальную автоматизированную систему распознавания биометрических образов по отпечаткам пальцев и рукописному почерку, которая показала достаточно высокую точность распознавания, и может быть использована для создания инструментальных средств.

Экономическая значимость полученных результатов достигается внедрением разработанной в диссертационной работе системы, использованием представленных методов и технологий в процессе автоматизации управленческих и инженерных задач.

Основные положения диссертации, выносимые на защиту.

– композитная нейросетевая модель, которая обеспечивает эффективное распознавание пользователей на основе анализа геометрических параметров фрагментов рукописного текста изменяемого размера;

– влияние корреляционных связей между выходными сигналами НС при оценке энтропии преобразователей биометрия-код;

– метод снижения входной выборки НС за счет учета корреляционных связей между выходными сигналами НС;

– архитектура автоматизированной интеллектуальной системы распознавания биометрических образов с использованием нейросетевых технологий;

– методика формирования баз рукописных образов и отпечатков пальцев.

Личный вклад соискателя. Основные положения и результаты диссертационной работы, выносимые на защиту, получены автором самостоятельно. В работах, написанных в соавторстве, личный вклад соискателя

заключается в следующем: [11] – проведены исследования по выявлению аномального состояния СОВ, [7, 9, 12, 13, 19] – проведен анализ технологий распознавания биометрических образов; [10, 14] – проведен анализ НС и выбор алгоритмов обучения; [3, 16, 17] – предложен метод снижения входной выборки НС за счет учета корреляционных связей между выходными сигналами НС; [1, 2] – предложен синтез хи-квадрат критерия для зависимых данных; [4-6, 8, 15] – проведено формирование баз рукописных образов и отпечатков пальцев.

Апробации результатов диссертации. Результаты исследований докладывались и обсуждались на семинарах кафедры «Информационная безопасность» КазНИТУ имени К.И. Сатпаева, кафедры «Информационные системы и технологии» КГТУ имени И.Раззакова, а также международных конференциях «Innovation Challenges In Multidisciplinary Research&Practice» (Kuala Lumpur, 2014), «Информационные и телекоммуникационные технологии: образование, наука, практика» (Алматы, 2015); «Інформаціина безпека та компютерні технологи» (Кировоград, 2016); Интеллектуальные информационные и коммуникационные технологии – средство осуществления третьей индустриальной революции в свете стратегии «Казахстан-2050» (Астана, 2017); «Актуальні питання забезпечення кібербезпеки та захисту інформації» (Киев, 2018).

Полнота отражения результатов диссертации в публикациях в журналах: «Известия КГТУ» (4 статьи); «Вестник НАН РК» (2 статьи); «Доклады НАН РК» (1 статья); «Journal of Theoretical and Applied Information Technology» (1 статья); «Захист информації» (1 статья); «Известия НАН РК» (1 статья), «Intelligent Systems in Cybernetics and Automation Control Theory» (1 статья), а также подтверждена 2 авторскими свидетельствами на программы.

Структура и объем диссертации. Диссертация состоит из введения, трех глав и приложений. Полный объем диссертации составляет 164 страницы, в том числе основного текста 136 страниц, включая 56 рисунков и 12 таблиц. Список использованной литературы состоит из 87 наименований.

ОСНОВНАЯ ЧАСТЬ

Во введении обоснована актуальность проблемы, сформулированы цель и задачи исследования, научная новизна и практическая ценность полученных результатов, приведены сведения об апробации работы и ее связи с государственными научно-техническими программами, дается информация о количестве публикаций.

В первой главе описываются интеллектуальные системы распознавания биометрических образов, базирующиеся на теории нейронных сетей.

Нейронные сети являются нелинейными. Это дает возможность использовать их самостоятельно или с другими традиционными методами. Они позволяют ослабить или вообще снять проблему «проклятия размерности», которая при большом количестве переменных не может смоделировать линейные зависимости. В случаях, когда необходимо сделать предварительный

анализ данных и найти зависимости между переменными нейронные сети показывают высокую эффективность. Анализируемые данные могут быть неполными, противоречивыми и даже искаженными. При существовании между входными и выходными данными какой-либо даже не обнаруживаемой корреляционными методами связи нейронная сеть может на нее настроиться. Кроме того, современные нейронные сети обладают следующими возможностями: позволяют уменьшить объем входной информации, сравнивая ее и сохраняя только существенные данные, прогнозировать на основе входных данных различные ситуации, в том числе и критические и т.д.

Резюмируя вышесказанное, можно сказать, что нейронные сети – это системы, которые на основе анализа входных данных, обучения сети дают результаты обработки, даже если на входе была плохо структурированная информация. Главным отличием нейронных сетей от других систем является то, что им не нужна заранее известная модель. Нейронные сети строят модель на основе входной информации. Поэтому их широко используют для решения задач классификации, прогнозирования, управления и, по сути, они являются базой для организации интеллектуальных систем защиты информации.

Существует различные примеры применения экспертных систем и систем поддержки принятия решений (интеллектуальных систем) для обеспечения информационной безопасности и кибербезопасности компьютерных систем [20, 21]. Одним из примеров интеллектуальных систем являются системы обнаружения вторжений (СОВ), которые позволяют анализировать, контролировать, прогнозировать и блокировать атаки. По методу обнаружения атак разделяют СОВ, базирующиеся на сигнатурном (шаблонном) и аномальном принципах обнаружения вторжений. Основная идея сигнатурного подхода заключается в описании атаки в виде шаблона (сигнатуры) и его поиска в контролируемом пространстве (например, в сетевом трафике, протоколах, журнале регистрации и др.). Системы второго типа ориентированы на обнаружение аномального поведения. Они содержат профиль нормального (ненормального) поведения системы и обнаруживают отклонения от него [11]. Эти СОВ основаны на том, что аномальное состояние системы проявляется как отклонение от нормального поведения с конкретным диапазоном значений переменных и состояний, а в аномальном случае необходимо учитывать более значительный диапазон изменения значений переменных и состояний.

Другим ярким примером применения нейронных сетей является защита информационных ресурсов автоматизированных систем от несанкционированного доступа, путем преобразования личных биометрических данных человека в его криптографический ключ. Криптографическая поддержка биометрических технологий является важнейшим моментом, обеспечивающим доверие к биометрическим данным. Все это становится особенно очевидным, когда речь идет о применении биометрии в Интернете и иных открытых информационных пространствах. В открытых информационных пространствах криптография является единственным эффективным способом защиты, то есть

необходимо осуществлять эффективное связывание биометрии с криптографией.

Существующие в настоящее время биометрические технологии распознавания образов делятся на три группы. К первой группе относятся технологии, основанные на анализе статических характеристик человека, а ко второй группе относятся технологии, основанные на анализе динамических характеристик человека. В третьей группе можно сочетать технологии первой и второй группы, то есть использовать мультибиометрические технологии. Были рассмотрены наиболее распространенные технологии распознавания как статических, так и динамических биометрических образов: отпечаток пальца, геометрия лица, сетчатка глаза, геометрия руки, рукописная подпись и голосовая фраза, каждая из которых имеет свои особенности, достоинства и недостатки. Из проведенного анализа следует, что статические методы по многим параметрам уступают динамическим. Во-первых, самая дешевая технология распознавания биометрических образов по отпечаткам пальцев стоит около $100, тогда как затраты на средства биометрические аутентификации по голосовой фразе и рукописному почерку гораздо ниже. Это обуславливается наличием аппаратных устройств ввода голосовой и рукописной информации в карманных компьютерах и смартфонах. Во-вторых, вероятность пропуска «Чужого» в статических метода высока по сравнению с динамическими. Например, для упомянутой выше технологии распознавания биометрических образов по отпечаткам пальцев она составляет порядка 10^{-6}. Стойкость же тайного пятибуквенного рукописного пароля биометрико-нейросетевой защиты для атаки среднестатистического пользователя находится на уровне 10^{9}.

В настоящей главе рассматривается технологии распознавания образов на основе модели нечетких экстракторов.

Для защиты биометрических кодов используют личный секретный криптографический ключ человека, к которому применяют избыточный самокорректирующийся код. Обычно применяют коды БЧХ (Боуза-Чоухуры-Хоквингема) и поэтому получают гамму в 10 раз длиннее секретного ключа. Далее к биометрическому коду применяют гамму для получения «нечеткого контейнера», который сохраняют для проведения процесса аутентификации. При проведении аутентификации вводят биометрический образ, оцифровывают его и гаммируют с сохраненным «нечетким контейнером» (рис.1).

«Нечеткие экстракторы» интересны тем, что позволяют в явной форме разделить стойкость криптографической защиты биометрического кода от наблюдения и стойкость биометрической защиты от атак подстановки случайных образов «Чужой». Стойкость криптографической защиты будет пропорциональна длине личного ключа, а биометрическая стойкость защиты пропорциональна длине биокода и показателям стабильности его разрядов.

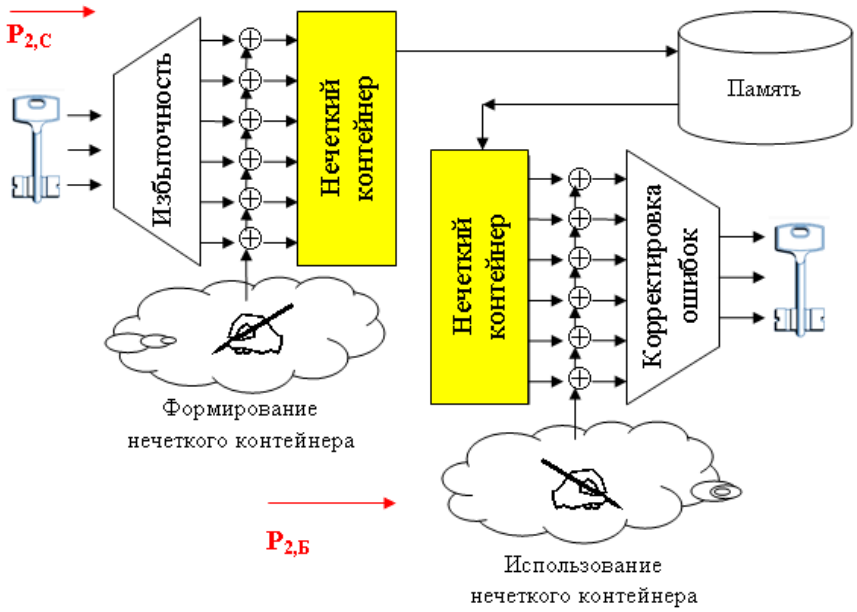

Рис.1. Схема работы «нечетких экстракторов» с гаммированием биометрического кода личности

Во второй главе рассматриваются модели и методы распознавания биометрических образов с использованием нейронных сетей.

В общем случае для распознавания любого биометрического образа необходимо преобразовать многомерный континуум биометрических данных образа «Свой» в код криптографического ключа доступа [12]. Для этого нужно отсканировать предъявленный биометрический образ, вычислить контролируемые биометрические параметры и предъявить их на вход преобразователя биометрия-код (рис. 2).

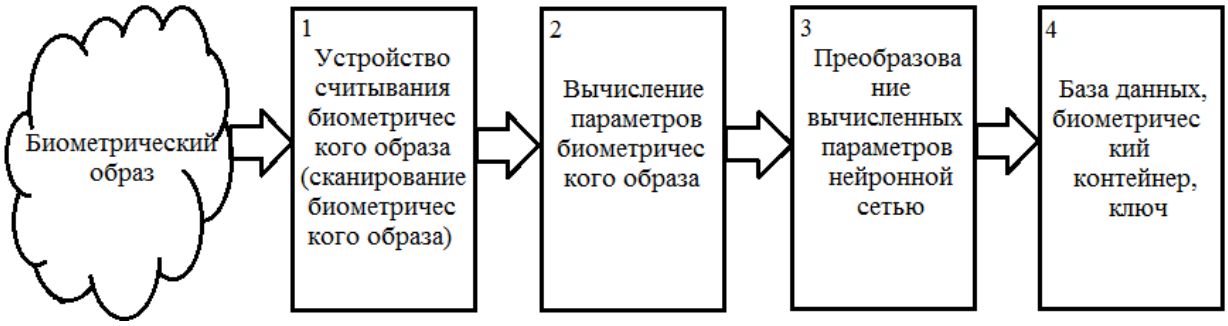

Рис. 2. Преобразование биометрических параметров в код ключа

В качестве анализируемых параметров рукописного почерка используются геометрические особенности текстовых фрагментов неопределенной длины. Предполагается, что на первом уровне распознавания нейронная сеть должна выделить элементарные признаки, представляющие собой четыре различным образом ориентированных отрезка, а также пустую и заполненную области.

Для построения нейросетевой модели использовалась хорошо апробированная и научно обоснованная методология разработки эффективных нейросетевых систем защиты информации, которая состоит из двух этапов:

- обоснование выбора наиболее эффективного вида модели;
- определение параметров модели эффективного вида.

При этом для обоснования выбора наиболее эффективного вида модели нами использован следующий принцип – наиболее эффективным является тот вид нейросетевой модели, характеристики которого наиболее полно соответствуют значимым условиям поставленной задачи защиты информации [10].

В базовом варианте предлагается разделить множество значимых условий на категории, характеризующие учебные данные, ограничения процесса обучения, вычислительные мощности, выходную информацию, техническую реализацию и сферу применения нейросетевых средств. Таким образом, задача выбора наиболее эффективного вида нейростевой модели сводится к задаче многофакторной оптимизации, описываемой выражением:

$$E_{\sum}(a_i) = \sum_{k=1}^{K} E_k(a_i) \to \max,\ a_i \in \mathrm{A},\ i = 1,2,...,I \qquad (1)$$

где $E_{\sum}$ - интегральный критерий оптимизации вида нейросетевой модели, a_i - i-ий вид нейросетевой модели, А, I - множество и количество допустимых видов нейросетевых моделей, E_k - k-ый критерий эффективности, K – количество критериев эффективности.

В результате проведения первого этапа было определено что, наиболее эффективными видами нейросетевых моделей являются сверточная нейронная сеть и рекурентная нейронная сеть долгой краткосрочной памяти. Наибольшие перспективы имеет нейросетевая модель, интегрирующая в себе возможности указанных типов сетей.

В процессе проведения второго этапа использовались четыре принципа адаптации структуры сверточной нейронной сети к задаче биометрической аутентификации пользователя на основании анализа двухмерной геометрии их биометрических образов, отображаемых в окне фиксированного размера. Кроме того был предложен еще один принцип адаптации: использование сверточных слоев не должно искажать геометрические параметры признаков, используемых для распознавания рукописных символов.

Адаптация значений параметров нейросетевой модели CNN-LSTM проводилась по блок-схеме указанной на рис. 3.

В результате проведения второго этапа были рассчитаны значения параметров нейросетевой модели CNN-LSTM: $a_0 = 33$, $L_{in} = 1089$, $K_{ls} = 2$, $L_{h,1} = 6$, $L_{h,2} = 24$, $(b \times b)_1 = (5 \times 5)$, $(b \times b)_2 = (5 \times 5)$, $d_1 = d_2 = 2$, $r_1 = r_2 = 0$, $a_1 = 15$, $a_2 = 6$ и определена структура адаптированной нейросетевой модели CNN-LSTM (рис. 4).

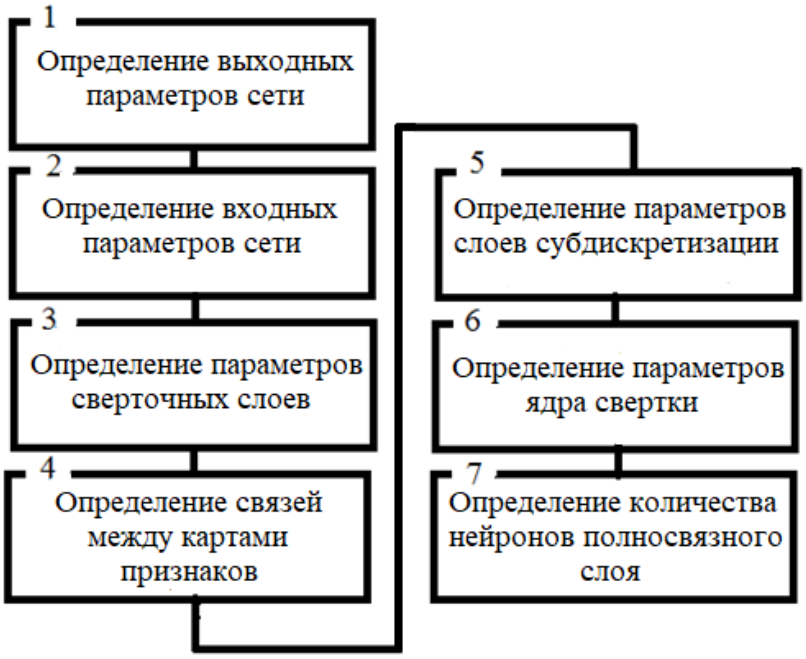

Рис. 3 – Укрупненная блок-схема алгоритма адаптации значений параметров CNN-LSTM

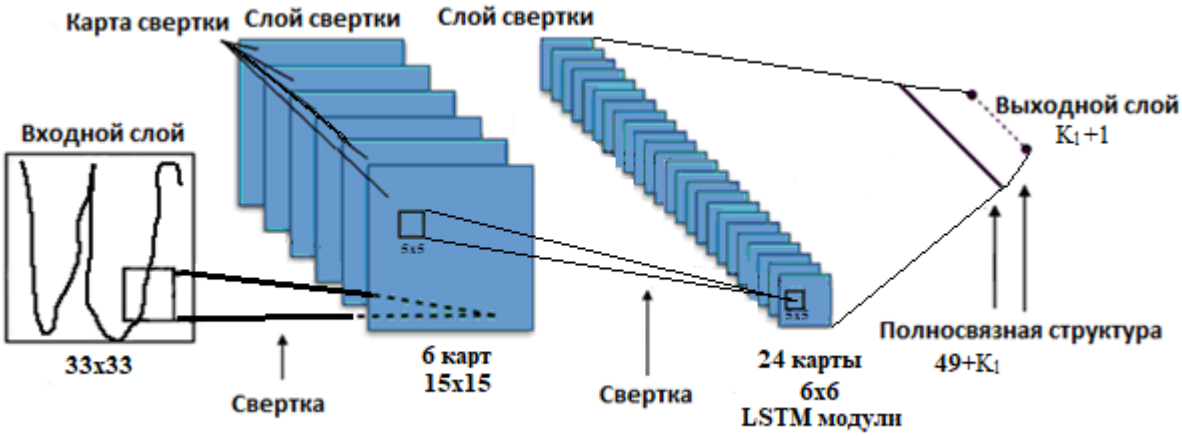

Рис. 4. Структура адаптированной нейросетевой модели CNN-LSTM

Обучение нейросетевой модели CNN-LSTM реализуется на базе общеизвестного алгоритма обратного распространения ошибки.

При работе с отпечатками пальцев необходимо получить биометрические параметры, которые будут инвариантны к размерности вектора контрольных точек и смещению пальца. Для этого сначала откорректируем координаты контрольных точек, затем используем двумерное дискретное ортогональное преобразование.

На этапе реализации преобразователя «биометрия-код» важным вопросом является выбор структуры нейронной сети. Для распознавания отпечатков пальцев ГОСТ Р 52633.5–2011 рекомендует однослойные или двухслойные нейронные сети. Для двухслойных нейронных сетей функции каждого слоя разделены. К функциям первого слоя относятся обогащение биометрических

данных и квантование обогащенных данных. Нейроны второго слоя при недостаточном обогащении исправляют ошибки биометрического кода нейронов первого слоя [13, 19].

Практические исследования показали, что большинство разрядов биометрического кода имеет высокую стабильность. Только некоторые разряды кода оказываются нестабильными и их положение известно [13, 19]. При обучении второй слой нейронов корректирует нестабильные разряды и одновременно хэширует все разряды биометрического кода.

После выбора количества слоев сети нужно выбрать количество входов каждого нейрона и задать связи входов с номерами входов сети. Нужное количество входов определяется непосредственно во время обучения нейрона. После обучения для каждого нейрона дополнительно получаем таблицу весовых коэффициентов входных связей [13].

Таблица весовых коэффициентов и таблица связей нейронов формально описывают обученную сеть. В двухслойных сетях эти таблицы создаются для каждого слоя нейронов. Слои нейронов обучаются последовательно. После обучения первого слоя нейронов примеры образов «Свой» и «Все Чужие» транслируются с входа НС на выходы нейронов. Таким образом, получают примеры биометрических кодов, на которых обучаются нейроны второго слоя [13].

В качестве алгоритма обучения был выбран абсолютно устойчивый не итерационный алгоритм обучения нейрона. Этот алгоритм строится на подборе значений весовых коэффициентов и их вероятных знаков для подбора ожидаемого решения. Это несколько снижает качество обучения, но ведет к появлению эффекта высокой устойчивости вычислений. Чем больше входов у обучаемого нейрона, тем выше устойчивость вычислений будет тем выше.

После обучения системы нам необходимо оценить качество обучения, то есть провести тестирование преобразователей биометрия-код. Для тестирования применяют N_1 векторов образов «Свой» и N_2 векторов образов «Чужой». На рис. 5 приведена схема тестирования системы.

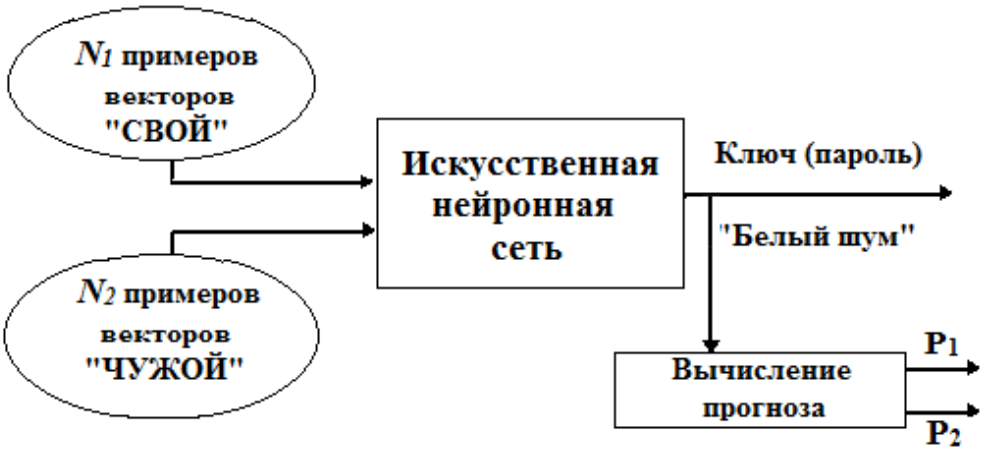

Рис. 5. Структурная схема тестирования системы биометрико-нейросетевой аутентификации

Любая биометрическая защита должна быть способна хорошо распознавать образ «Свой» и надежно выделять множество образов «Чужой» («Все Чужие»). Очевидно, что средство биометрической защиты может ошибаться. Основной и первой задачей для биометрии является обеспечение доступа донору биометрического образа «Свой». Ошибка при выполнении этой задачи называется ошибкой первого рода. Вероятность появления ошибки первого рода P_1 является основной характеристикой эффективности работы системы.

Второй задачей средства биометрической аутентификации является препятствовать доступу донору образа «Чужой». Если придерживаться гипотезы нормальности закона распределения значений показателей критерия Хэмминга, то можно вычислить математическое ожидание распределения данных распределения p(h(x)) и его среднеквадратическое отклонение. Приближенную оценку вероятности ошибки второго при тестировании можно вычислить по следующей формуле:

$$P_2 \approx \frac{1}{\sigma(h(x)) \cdot \sqrt{2\pi}} \int_0^{\max(h(c))} \exp\left\{ \frac{-(E(h(x)) - u)^2}{2 \cdot \sigma^2(h(x))} \right\} \cdot du \ , \qquad (2)$$

где max(h(c)) – максимально возможное значение расстояние Хэмминга кодов «Свой»; E(h(x)) – математическое ожидание расстояний Хэмминга кодов «Чужие»; σ(h(x)) – среднеквадратичное отклонение расстояний кодов «Чужие».

На практике часто пользуются понятием стойкости преобразователя биометрия-код, которая обратно пропорциональна его вероятности ошибки второго рода.

Сложность распознавания биометрических образов вызвана многими причинами, одной которых является высокая размерность задачи. То есть, приходится учитывать множество «плохих» биометрических параметров, поэтому невозможно воспользоваться классической линейной алгеброй и многомерной статистикой. Учет дополнительных биометрических параметров не приводит к более точным результатам, однако все происходит с точностью до наоборот. Происходит накопление погрешностей вычислений. Именно из-за этой ситуации, известной как «проклятие размерности», в биометрии не удается пользоваться линейной алгеброй и классической многомерной статистикой [15]. Ослабить проблему «проклятия размерности» или вообще снять позволяет применение ИНС.

В работе показано, что реальная размерность решаемой задачи распознавания образов связана со значением выходной энтропии кодовых состояний преобразователя биометрия-код, полученная воздействием на него образами «Все Чужие».

У кода длиной 256 бит энтропия H будет равна 256 битам. Энтропия будет падать, если код будет не случайным [16]:

$$H(256) \langle 256 \text{ при } \left|r_{i,j}\right| \rangle 0.0 \text{ хотя бы для одной пары } i \neq j. \qquad (3)$$

Для всех кодов с коррелированными и независимыми разрядами энтропия связана с показателем стойкости к атакам подбора или с вероятностью ошибок второго рода P_2. В общем виде можно записать:

$$H(n) = -\log_2(P_2), \qquad (4)$$

где n – длина биометрического кода; P_2 – вероятность ошибки второго рода преобразователя биометрия-код.

Важным моментом при этом является вопрос вычисления энтропии выходных биометрических кодов [3]. Классический метод вычисления многомерной энтропии с использованием формулы Шеннона

$$H(256) = -\sum_{i=1}^{2^{256}} P_i \cdot \log_2(P_i), \qquad (5)$$

где P_i – вероятность появления i-го состояния биокода, требует больших вычислительных затрат и размеров исходных биометрических данных.

Одним из вариантов значительного снижения объемов вычислений является переход из поля обычных кодов в поле кодов расстояний Хэмминга.

Если выходной код представить в виде двоичного вектора $\bar{x}$, то мера Хэмминга до кода «Свой» $\bar{c}$ вычисляется по формуле [16]:

$$h = \sum_{i=1}^{256} x_i \oplus c_i, \qquad (6)$$

где 256 – длина сравниваемых кодов; I – номер сравниваемых разрядов; $\oplus$ – операция сложения по модулю два.

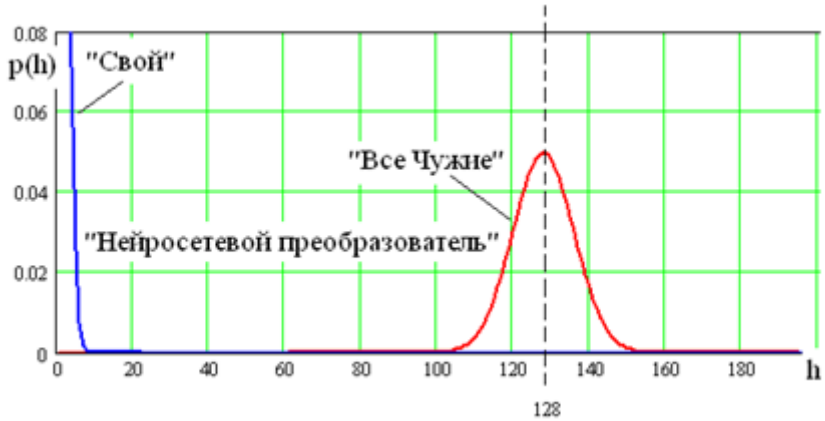

Рис. 6. Распределение расстояний Хэмминга для кодов длиной 256 бит

На рис. 6 [14, 15] показано вычисленное распределение расстояний Хэмминга между выходными кодами «Чужие» и выходным кодом «Свой». Для

кодов «Свой» мера Хэмминга сжимается (прижимается к оси системы координат), так как применение нейросетевых преобразователей дает возможность улучшать их качество и нестабильность на выходе преобразователя доходит до 7 бит.

Еще одной важной особенностью распределения Хэмминга кодов «Все Чужие» является то, что оно очень хорошо описывается нормальным законом распределения значений. Это позволяет рассчитать ожидаемую вероятность ошибок второго рода по формуле (2).

Далее, вычисляя энтропию выходных кодов по формуле (4), мы фактически уменьшаем длину выходного кода до полноценной размерности задачи, рассматривая разницу между длинами кода. При таком методе оценки размерность решаемой биометрической задачи может быть очень высокой даже при относительно малых длинах выходного кода, если его разряды слабо коррелированны. При росте корреляционных связей между разрядами кода размерность решенной задачи биометрической защиты падает.

Для проверки статистических гипотез во многих областях исследований применяют хи-квадрат критерий, и биометрия не является исключением. При высокой коррелированности данных использовать критерий хи-квадрат нельзя, по причине того, что он работает только в рамках предположения независимости. Чтобы решить этот вопрос была разработана методика синтеза хи-квадрат распределений зависимых данных [1, 2].

В работе показано, что число степеней свободы хи-квадрат распределения зависимых данных и их математические ожидания имеют точное совпадение. Это свойство работает для любых коэффициентов равной коррелированности. С повышением коррелированности данных происходит частичная утрата количества степеней свободы [1, 2]. Зная число степеней свободы и соответствующий ей коэффициент равной коррелированности данных можно увеличить достоверность оценок проверки статистических гипотез.

В третьей главе приведена разработанная методика формирования биометрической базы естественных рукописных образов и папиллярных рисунков отпечатков пальцев, описана разработанная интеллектуальная автоматизированная система распознавания рукописных образов и рисунков отпечатков пальцев, проведено ее экспериментальное исследование.

Чтобы провести достоверное тестирование требуются небольшие базы биометрических образов «Свой» и большие базы биометрических образов «Чужой» (свыше 10^{12} образов) [4, 8]. Если формирование баз «Свой» не вызывает затруднений, то формирование баз «Чужой» требует больших затрат времени и труда. Выходом из данного положения является использование усеченных баз «Чужой», содержащих 10^3–10^5 образов, полученных в рамках работы системы [4].

Имеющиеся базы можно дополнять с помощью специальных технологий, например, путем случайного выбора людей и получением от них случайных образов, что вполне возможно для сбора рукописных паролей.

В главе дается классификация пользователей, которые могут классифицироваться по стабильности их биометрических образов и уникальности их биометрических параметров.

В первом случае для формирования классификации необходимо оценить стабильность пользователей и построить их нормированное распределение показателя стабильности (рис. 7).

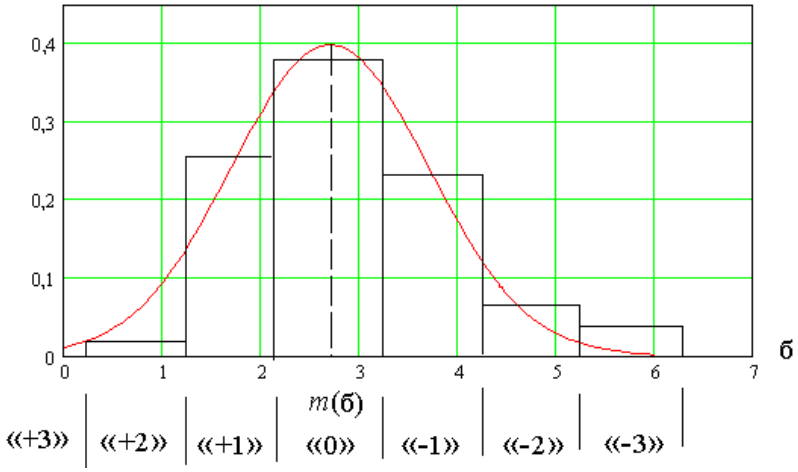

Рис. 7. Экспериментально полученное распределение пользователей по стабильности их биометрических образов

Столбцы гистограммы соответствуют классу стабильности пользователей. Для проведения классификации распределение «Все Свои» было разделено на интервалы, которые равны дисперсии, а центром интервала было математическое ожидание. В итоге была получена классификация стабильности «+3», «+2», «+1», «0», «–1», «–2», «–3». Классификация должна строиться только для дееспособных людей.

Во втором случае рассматривается уникальность биометрического образа «Свой», которая является важной характеристикой систем биометрической защиты. Очевидно, что злоумышленник всегда будет стараться выбирать при атаках подбора наиболее вероятные состояния входов биометрической защиты, то есть злоумышленник имеет модель среднестатистического «Своего» (или модель «Все чужие») и будет стараться использовать ее при организации атак. Естественно, что чем больше образ «Свой» будет отличаться от среднестатистического образа, тем выше степень биометрической защиты. Уникальность может быть применена для классификации биометрических образов, которая проводится с помощью статистического исследования большого количества биометрических образов.

Очевидно, что у разных биометрических образов разная информативность (сложность). Очень простые биометрические образы легко подбираются и не могут обладать сколько-нибудь существенной стойкостью. Чем сложнее биометрический образ, тем сложнее его подбор. Это непреложное правило справедливо для любых статических или динамических биометрических образов. Стойкость биометрических образов зависит от их информативности

(сложности), поэтому при формировании баз биометрических образов необходимо выбирать длину слов–паролей не менее чем из 5 букв, а при использовании отпечатков пальцев использовать не менее 22 особенностей.

В главе дается классификация баз естественных биометрических образов, которые могут делиться в зависимости от типа биометрического образа, технологии преобразования биометрического образа, признака «Свой» – «Чужой», динамических биометрических образов «Чужой» в соответствии со степенью компрометации тайны биометрического образа «Свой», биометрических образов «Свой» и области применения.

Сформулированы требования к техническому и программному обеспечению автоматизированного формирования базы биометрических тестовых образов.

Были разработаны требования к формированию баз естественных биометрических рукописных образов «Свой» и «Чужой», предназначенных для тестирования средств биометрического распознавания.

Также были определены требования к донорам биометрии и безопасному использованию их биометрических образов.

На основе сформированных требований разработаны методики формирования биометрической базы естественных рукописных образов и папиллярных рисунков отпечатков пальцев, в соответствии с которыми определен порядок формирования биометрических баз.

Сбор биометрических образов осуществляется в три этапа.

Первый этап – отбор доноров биометрии. Биометрические образы должны быть получены от доноров, которые могут пользоваться биометрическими средствами, поэтому этот этап является обязательным [5].

Второй этап – обучение донора и создание базы биометрических образов «Свой». К обучению доноров относиться освоение донором программы, устройства ввода, выработка навыков стабильного написания рекомендуемого слова. При создании базы биометрических образов «Свой» донор должен ввести 40 образов предложенного слова. На данном этапе контролирующее лицо должен следить за действиями донора, вести протокол и при необходимости требовать от донора повторного ввода биометрического образа.

Третий этап – формирование базы биометрических образов «Чужой». На этом этапе донор должен воспроизводить на устройстве считывания, задаваемые программным модулем слова. Программный модуль задает разные слова длиной от пяти до семи букв, которые необходимо писать один раз.

Рекомендуемое нами время на формирование баз «Свой» и «Чужой» по разработанной методике не должно быть больше 80 минут [6]. Увеличение времени приводит к ухудшению качества вводимых рукописных образов.

Формирование биометрической базы отпечатков пальцев осуществляется аналогично.

В главе описывается интеллектуальная система распознавания образов.

Система реализует следующий функционал: формирование тестовой рукописной базы образов и базы рисунков отпечатков пальцев; распознавание

рукописных образов и рисунков отпечатков пальцев; тестирование системы распознавания биометрических образов с использованием сформированных баз рукописных почерков и баз рисунков отпечатков пальцев.

Система включает следующие модули и программы [17, 18]:

1) программно-аппаратный комплекс «Нейро-Тест 1.2», который предназначен для обучения и тестирования средства биометрико-нейросетевой аутентификации личности по рукописному слову-паролю. Он включает в себя компьютер, графический планшет, программный модуль «Нейрокриптон-формирователь биометрических баз».

2) программный модуль «Нейрокриптон – формирователь биометрических баз» включает следующие модули и словари:

– **BioImgDBCreator.exe** – модуль предназначен для сбора тестовых рукописных образов «Свой» и «Чужой»;

– AlmatyTurkestanPenza.exe – модуль предназначен для сбора баз близких образов;

– **bnc32.dll** – биометрико-нейросетевая библиотека, поддерживающая работу нейронных сетей (моделирование, обучение, тестирование). Программа автоматически предлагает донору биометрии слова для воспроизведения на графическом планшете из словарей: **diction_full.txt** и **Almaty_Turkestan_Penza.txt;**

– словарь **diction_full** представляет из себя текстовый документ, содержащий 10 000 слов длиной от 4 до 6 букв на казахском языке;

– словарь **Almaty_Turkestan_Penza.txt** представляет из себя текстовый документ, содержащий 597 слов.

3) программно-аппаратный модуль формирования базы естественных биометрических образов папиллярных рисунков отпечатков пальцев. Он обеспечивает обучение пользователя и контроль корректного ввода образов, загрузку и визуальную проверку ранее созданной базы. Для сбора отпечатков пальцев необходимо подключить сканер отпечатков пальцев Futronic FS80 и установить соответствующий драйвер. Вся последовательность действий по формированию баз отпечатков пальцев подробно описана в диссертации.

4) модуль регистрации биометрических данных отпечатка пальца, обучения нейронной сети распознаванию биометрического образа «Свой», аутентификации по отпечатку пальца.

5) модуль тестирования стойкости преобразований к атакам, направленным на подбор выходного кода нейронной сети.

В работе было проведено экспериментальное тестирование разработанной интеллектуальной автоматизированной системы распознавания биометрических образов, а именно:

– сформирована тестовая рукописная база образов;

– проведено тестирование системы распознавания биометрических образов с использованием сформированных баз рукописных почерков. Результаты экспериментов показали величину ошибки второго рода в пределах 10^{-15};

– сформирована тестовая база папиллярных рисунков отпечатков пальцев;

– проведено тестирование системы распознавания биометрических образов с использованием сформированных баз папиллярных рисунков отпечатков пальцев. Результаты экспериментов показали величину ошибки второго рода в пределах 10^{-4}.

Также в главе приведены результаты сравнительного анализа разработанной системы распознавания образов с аналогами, который проводился по скорости тестирования и стойкости (величине ошибки второго рода). Результаты приведены в таблице 1.

Таблица 3.5 - Сравнительный анализ систем распознавания образов

Количество образов	Mnist_brain-master		Нейротест 1.1		Нейротест 1.2	
	Скорость тестирования (сек)	Точ-ность (P_2)	Скорость тестирова-ния (сек)	Точ-ность (P_2)	Скорость тестирова-ния (сек)	Точ-ность (P_2)
1000	0,0	10^{-13}	0,0	10^{-17}	0,0	10^{-17}
10000	0,58	10^{-13}	0,36	10^{-15}	0,24	10^{-16}
25000	3,13	10^{-12}	1,27	10^{-15}	0,59	10^{-15}
50000	13,06	10^{-10}	5,19	10^{-13}	3,02	10^{-14}
100000	37,41	10^{-8}	12,53	10^{-11}	7,46	10^{-12}

Сравнительный анализ показал, что разработанная нами система выигрывает по времени тестирования и по величине ошибок второго рода. Все три системы имеют высокую масштабируемость, так как имеют высокую скорость распознавания.

ВЫВОДЫ

1. Разработана композитная нейросетевая модель, которая за счет использования в сверточной нейронной сети модулей долгой краткосрочной памяти, а также за счет адаптации параметров модели к условиям системы биометрической аутентификации, позволяет с точностью 10^{-15} реализовать распознавание пользователей на основе анализа геометрических параметров фрагментов рукописного текста изменяемого размера;
2. Исследовано влияние корреляционных связей между выходными сигналами нейронных сетей при оценке энтропии преобразователей биометрия-код;
3. Предложен метод снижения входной выборки нейронной сети за счет учета корреляционных связей между выходными сигналами нейронных сетей;
4. Разработана архитектура автоматизированной интеллектуальной системы распознавания биометрических образов с использованием нейросетевых технологий;
5. Разработана методика формирования баз рукописных образов и отпечатков пальцев.
7. Результаты исследований были реализованы в виде:

– интеллектуальной автоматизированной системы распознавания рукописных образов «Нейротест 1.2» с использованием нейросетевых технологий;

– программно-аппаратного комплекса биометрико-нейросетевой аутентификации личности по отпечаткам пальцев FINGER;

– специальной методики формирования баз рукописных образов и отпечатков пальцев.

ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ

Результаты исследований использованы в:

– ТОО «QUARES» (Казахстан, Алматы);

– НИЦ «Тезис» КПИ имени И. Сикорского (Украина, Киев);

– учебном процессе кафедры «Информационная безопасность» КазНИТУ имени К.И. Сатпаева (Казахстан, Алматы);

– учебном процессе кафедры «Безопасность информационных технологий» Национального авиационного университета (Украина, Киев);

– в учебнике «Қолданбалы криптология: шифрлау әдістері», рекомендованным Министерством образования и науки РК.

На разработанную интеллектуальную автоматизированную систему распознавания рукописных образов «Нейротест 1.2» было получено авторское свидетельство № 1240 от 08.01.2019 года.

На разработанный программно-аппаратный комплекс биометрико-нейросетевой аутентификации личности по отпечаткам пальцев FINGER было получено авторское свидетельство № 1287 от 11.01.2019 года.

Результаты диссертации могут использоваться:

- для распознавания других биометрических образов как статических, так и динамических;

- для внедрения в готовые системы, как модуль высоконадежной биометрико-нейросетевой аутентификации.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. **Akhmetov, B. S.** Criterion synthesis the chi-square for dependent data [Текст] / B. S. Akhmetov, Zh. K. Alimseitova, N. I. Serikova, A. I. Ivanov, Yu. V. Foontikova // 2nd International Conference on Innovation Challenges In Multidisciplinary Research & Practice. – Kuala Lumpur, Malaysia, 2014. – P. 64–70.
2. **Ахметов, Б.С**. Синтез критерия хи-квадрат для зависимых данных [Текст] / Ж. К. Алимсеитова, Н. И. Серикова, А. И. Иванов, Ю. В. Фунтикова // Труды международного форума «Инженерное образование и наука в XXI веке: проблемы и перспективы», посвященной 80-летию КазНТУ имени К.И. Сатпаева – Алматы, 2014. – Том II. – С. 368-372.
3. **Иванов, А. И.** Вычисление энтропии слабо коррелированных и сильно коррелированных длинных биометрических кодов на малых тестовых выборках [Текст] / А. И. Иванов, Б. Б. Ахметов, А. В. Безяев, К. А. Перфилов, Ж. К. Алимсеитова // Вестник НАН РК. Алматы. 2015. – №3. – С. 64-70.
4. **Ахметов, Б. С.** Методика формирования баз биометрических образов [Текст] / Б. С. Ахметов, Н. А. Сейлова, Ж. К. Алимсеитова, А. Балтабай // Сборник материалов Всероссийской научно-практической конференции «Информационно-телекоммуникационные системы и технологии». Кемерово. 2015. [Электронный ресурс] – Режим доступа: http://sibscience.ru/page/ITSIT-2015/ITSIT/3-Prikladnye-informacionnye-tehnologii/PIT.html
5. **Ахметов, Б. С.** Формирование биометрической базы рукописных образов на казахском языке для программ биометрической аутентификации личностей [Текст] / Б. С. Ахметов, Ж. К. Алимсеитова, А. И. Малыгин, Х. И. Юбузова // Труды II Международной научно-практической конференции «Информационные и телекоммуникационные технологии: образование, наука, практика». Алматы: КазНИТУ им. К.И.Сатпаева. 2015. – Том II. – С. 32-35.
6. **Akhmetov, B. S.** Methodology of biometric image databases formation [Текст] / B. S. Akhmetov, N. A. Seilova, Zh. K. Alimseitova, A. Baltabay // First International Conference ISPIT 2015: Conference proceedings information security and protection of ingormation technology. St. Petersburg: Russia. 2015. – С. 48-52.
7. **Боскебеев, К. Дж.** Информационная система обработки цифровой информации для идентификации объекта [Текст] / К. Дж. Боскебеев, Ж. К. Алимсеитова // Известия Кыргызского государственного технического университета им. И. Раззакова. Бишкек. 2016. – № 1(37).– С. 8-12.
8. **Ахметов, Б. С.** Высоконадежная аутентификация: требования к базам биометрических образов [Текст] / Б. С. Ахметов, Ж. К. Алимсеитова, А. Картаев // Збірник тез доповідей міжнародна науково-практична конференція "Інформаціина безпека та компютерні технологи" InfoSec & CompTech 24-25 березня. Кировоград. 2016. – С. 11-12
9. **Алимсеитова, Ж. К.** Идентификация личности по рукописному почерку [Текст] / Ж. К. Алимсеитова, Н. А. Сейлова // Сборник материалов III Международной научно-практической конференции "Фундаментальные

научные исследования: теоретические и практические аспекты". Кемерово: Западно-Сибирский научный центр. 2017. – С.188-190

10. **Ахметов, Б.** Определение оптимального типа нейросетевой модели для биометрической аутентификации [Текст] / Б. Ахметов, Л. Терейковская, И. Терейковский, Ж. Алимсеитова // Сборник трудов IV Международной научно-практической конференции «Интеллектуальные информационные и коммуникационные технологии – средство осуществления третьей индустриальной революции в свете Стратегии «Казахстан-2050»» посвященной 70-летию профессора М. Бейсенби. Астана: ЕНУ им. Л.Н. Гумилева. 2017. – С. 155-157

11. **Ахметов, Б.** Система выявления аномального состояния в информационных системах [Текст] / Б. Ахметов, А. Корченко, Ж. Алимсеитова, Н. Жумангалиева. Доклады НАН РК. Алматы. 2017. – №5. – С. 28-37.

12. **Алимсеитова, Ж.** Технологии распознавания образов с использованием биометрии личности [Текст] / Ж. Алимсеитова, К. Дж. Боскебеев // Известия Кыргызского государственного технического университета им. И. Раззакова. Бишкек. 2017. – № 1(41). – Часть 2. – С. 11-17.

13. **Алимсеитова, Ж.** Анализ использования технологий распознавания биометрических образов [Текст] / Ж. Алимсеитова, Ж. З. Акматалиева, К. Дж. Боскебеев // Известия Кыргызского государственного технического университета им. И. Раззакова. Бишкек. 2017. – № 2(42). – С.14-19.

14. **Malygin, A.** Application of artificial neural networks forhandwritten biometric images recognition [Текст] / A. Malygin, N. Seilova, K. Boskebeev, Zh. Alimseitova // Journal “Computer modeling and Technologies”. Riga. 2017. – volume 21, №1. – С.14-19.

15. **Ахметов, Б.** Применение искусственных нейронных сетей для распознавания биометрических образов [Текст] / Б. Ахметов, Н. Сейлова, К. Боскебеев, Ж. Алимсеитова // Вестник НАН РК. Алматы. 2017. – №6 – С.75-84.

16. **Алимсеитова, Ж.** Проблемы размерности задач распознавания образов и пути их решения [Текст]: / Ж. Алимсеитова, Н. Сейлова, С. Гнатюк // Захист информації. Киев. 2017. – том 19. – №4. – С. 310-316. DOI: 10.18372/2410-7840.19.12219

17. **Akhmetov, B. S.** Training of neural network biometry-code converters [Текст] / B. S. Akhmetov, A. I. Ivanov, Zh. K. Alimseitova // Известия НАН РК. Серия геология и технические науки. Алматы. 2018. – №1(427). – С. 61-68.

18. **Алимсеитова, Ж.** Программно-аппаратный модуль распознавания рукописных образов [Текст] / Ж. Алимсеитова // Известия Кыргызского государственного технического университета им. И. Раззакова. Бишкек. 2018. - № 1(45) – С. 11-19.

19. **Алимсеитова, Ж.** Система распознавания биометрических образов [Текст] / Ж. Алимсеитова, К. Боскебеев // Тези доповідей участників iv міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації». Киев. 2018. – С. 23-24.

20. **Lakhno, V.** Development of a decision support system based on expert

evaluation for the Situation Center of Transport Cybersecurity [Текст] / V. Lakhno, B. Akhmetov, A. Korchenko, Z. Alimseitova, V. Grebenuk. Journal of Theoretical and Applied Information Technology. 2018. – Vol. 96. – № 14 – P. 4530-4540.

21. **B. Akhmetov.** Development of Sectoral Intellectualized Expert Systems and Decision Making Support Systems in Cybersecurity [Текст] / B. Akhmetov, V. Lakhno, B. Akhmetov, Z. Alimseitova // Intelligent Systems in Cybernetics and Automation Control Theory. CoMeSySo 2018. Advances in Intelligent Systems and Computing. – Vol 860. – P.162-171.

Авторские свидетельства

22. Свидетельство о внесении сведений в государственный реестр прав на объекты, охраняемые авторскими правами № 1240 от 09.01.2019г. Республика Казахстан. Нейротест 1.2 [Текст] / Ж. К. Алимсеитова, Т. С. Картбаев, Б. С. Ахметов, А. А. Досжанова.

23. Свидетельство о внесении сведений в государственный реестр прав на объекты, охраняемые авторскими правами № 1287 от 11.01.2019г. Республика Казахстан. Программно-аппаратный комплекс биометрико-нейросетевой аутентификации личности по отпечаткам пальцев FINGER [Текст] / Ж. К. Алимсеитова, Б. С. Ахметов, Т. С. Картбаев, А. А. Досжанова, Ш. Д. Толыбаев.

Учебник

24. Қолданбалы криптология: шифрлау әдістері [Текст] / [Б. С. Ахметов, А. Г. Корченко, В.П. Сиденко и др.]. – Алматы: КазНИТУ имени К.И. Сатпаева, 2016. – 500 с.

РЕЗЮМЕ

диссертации Алимсеитовой Жулдыз Кенесхановны на тему **«Разработка интеллектуальной автоматизированной системы распознавания биометрических образов»** на соискание ученой степени кандидата технических наук по специальности 05.13.16 – «Применение вычислительной техники, математического моделирования и математических методов в научных исследованиях».

Ключевые слова: информационная безопасность, интеллектуальные системы, биометрические образы, биометрическая аутентификация, нейронные сети, биометрико-нейросетевые технологии защиты информации.

Диссертационная работа посвящена вопросам повышения эффективности распознавания биометрических образов в информационных системах на основе использования биометрико-нейросетевых методов.

В работе поставлены и решены следующие основные задачи:

– разработана композитная нейросетевая модель, которая за счет использования в сверточной нейронной сети модулей долгой краткосрочной памяти, а также за счет адаптации параметров модели к условиям системы биометрической аутентификации, обеспечивает эффективное распознавание пользователей на основе анализа геометрических параметров фрагментов рукописного текста изменяемого размера;

– исследовано влияние корреляционных связей между выходными сигналами нейронных сетей при оценке энтропии преобразователей биометрия-код;

– предлагается метод синтеза критерия хи-квадрат распределений зависимых данных, позволяющий существенно увеличить достоверность оценок проверки статистических гипотез;

– разработана архитектура автоматизированной интеллектуальной системы распознавания биометрических образов с использованием нейросетевых технологий;

– разработана методика формирования баз рукописных образов и отпечатков пальцев.

Результаты в виде специального аппаратно-программного средства были апробированы в ТОО «QUARES» (Алматы), НИЦ «Тезис» КПИ имени И.Сикорского (Украина, Киев) и показали высокую эффективность распознавания биометрических образов. Также результаты диссертационного исследования используются в учебном процессе кафедры «Информационная безопасность» КазНИТУ имени К.И.Сатпаева (Алматы) и кафедры «Безопасность информационных технологий» Национального авиационного университета (Украина, Киев).

РЕЗЮМЕ

Алимсеитова Жулдыз Кенесхановнанын диссертациянын темасында **«Биометрикалык сүрөттөрүдү таануу, интеллектуалдык автоматташтырылган системаны иштеп чыгуу»** окумуштуулук даражасын изденип алуу үчүн талапкер техникалык илимдер адистиги боюнча 05.13.16 - «Илимий изилдөөлөрдө, математикалык моделдөөнү жана математика методдорун эсептөө техникасында колдонуу»

Негизги сөздөр: маалыматтык коопсуздук, акылдуу системалар, биометрикалык сүрөттөр, биометрикалык аныктыгын текшерүү, нейрон тармактары, биометрикалык-нейрон тармак маалыматын коргоо технологиясы.

Биометрикалык сүрөттөрү таануунун натыйжалуулугун жогорулатуу, биометрикалык-нейрон тармак ыкмаларын пайдалануу менен маалымат тутумдардын диссертациянын жумушунун маселесине арналган.

Ишине коюлган жана төмөнкү чечилген негизги милдеттерди аткарат:

- бакубатта жана кыска узак мөөнөттүүндө эстутумга, бир сверточной нейронтармак модулдары менен, жана биометрикалык тастыктоо системасынын шарттарына модель параметрлерин алмаштыруу аркылуу, өзгөрмө колжазма геометриялык параметрлери сыныктары талдоого негизделген пайдалануучулардын натыйжалуу таанууну камсыз курама нейрон тармак моделин иштеп чыккан;
- корреляционндук байланыштын таасирин изилдөөдө ортосундагы нейронндук тармактарын чыгуу сигналдарынын энтропии балоодогу өзгөруулөрдүн биометрия-коду.
- хи-квадраттын бөлүштүрүү көз каранды маалыматтарды синтез ыкмасын сунуштайт, статистикалык гипотездин текшерүүнүн ишенимдүүлүгүн жогорулатуу мүмкүн олуттуу баанын аныктыгын көбөйтүүсүн аныктайт.
- нейрон тармак технологиясын колдонуп биометрикалык үлгү таануу автоматташтырылган интеллектуалдык системасынын архитектурасы иштелип чыккан;
-манжалардын тактарын жана кол жазма сүрөттөрдүн негиздерин түзүүнүн методикасы иштелип чыккан.

Аппараттык-программалык каражаттар атайын текшерүүдөн өтүүгө ОШОЛ "QUARES" (Алматы), УМБ "Тезис" КПИ И. Сикорский атындагы (Украина, Киев) жана биометрикалык үлгү таанууну жогорку натыйжалуулугун корсоттуу. Ошондой эле, диссертациялык изилдөөнүн натыйжасы, окуу процессинде "Маалымат коопсуздугу" кафедрасанда пайдаланылат КазНИТУ К. И. Сатпаева атындагы (Алматы) жана «Коопсуздукту сактоо маалыматтык технологиялар» кафедрсы Улуттук авиациялык университети (Украина, Киев) колдонулат.

SUMMARY

of the dissertation work by Zhuldyz Alimseitova on the theme **«Development of intelligent automated system for biometric image recognition»** for the scientific degree of candidate of technical sciences on specialty 05.13.16 – «Application of computer technology, mathematical modeling and mathematical methods in scientific research».

Key words: information security, intellectual systems, biometric images, biometric authentication, neural networks, biometric neural network information security technologies.

The dissertation work is devoted to the problems of increasing the efficiency of biometric images recognition in information systems based on the use of biometric neural network methods.

The following main tasks are set and solved in the work:

- a composite neural network model has been developed, which due to the use of long-term memory modules in the convolutional neural network, as well as due to the adaptation of the model parameters to the conditions of the biometric authentication system, provides effective user recognition based on the analysis of the geometric parameters of handwritten text fragments of variable size;
- investigated the influence of correlations between the output signals of neural networks evaluating the entropy of biometry-code converters;
- the method of synthesis of the Chi-square criterion of dependent data distributions is proposed, which allows to significantly increase the reliability of statistical hypothesis testing estimates;
- developed the architecture of the automated intellectual system of biometric images recognition with use of neural network technologies;
- developed the method of hand-written images and fingerprints bases formation.

The results of the implementation in the form of a special hardware and software were tested at «QUARES» LLP (Almaty), at SRC «Thesis» of KPI named after I. Sikorsky (Ukraine, Kiev) and showed high biometric images recognition efficiency. Also, the results of the dissertation research are used in the educational process of the Information Security Department of KazNRTU named after K.I.Satpayev and of the Information Technology Security Department of the National Aviation University (Ukraine, Kiev).