УДК 004.93'1
doi:10.31799/1684-8853-2024-2-21-38
EDN: YIVAYM

Научные статьи
Articles

Аутентификация по голосовым паролям с обеспечением конфиденциальности биометрических данных на основе корреляционных нейронов

А. Е. Сулавко[а], *канд. техн. наук, доцент, orcid.org/0000-0002-9029-8028, sulavich@mail.ru*
Д. П. Иниватов[а], *ассистент, orcid.org/0000-0001-9911-1218*
В. И. Васильев[б], *доктор техн. наук, профессор, orcid.org/0000-0002-6105-5481*
П. С. Ложников[а], *доктор техн. наук, профессор, orcid.org/0000-0001-7878-1976*
[а]*Омский государственный технический университет, Мира пр., 11, Омск, 644050, РФ*
[б]*Уфимский университет науки и технологий, Заки Валиди ул., 32, Уфа, 450076, РФ*

Введение: *вопрос защиты биометрических данных от компрометации тесно связан с вопросами производительности. Существующие методы биометрической аутентификации по голосу либо не позволяют защитить голосовые данные от компрометации, либо дают высокий процент ошибочных решений и, кроме того, не гарантируют устойчивость к дрейфу голосовых образов.* ***Цель:*** *разработать метод биометрической аутентификации по голосу, устойчивый к дрейфу биометрических данных, с обеспечением конфиденциальности параметров голоса.* ***Результаты:*** *предложен метод аутентификации с использованием нейросетевых преобразователей биометрия-код на базе модифицированной модели корреляционных нейронов и алгоритмов их обучения. Вычислительный эксперимент показал, что корреляционные связи между признаками содержат информацию об образах, которая не дублирует информацию, содержащуюся в признаках. Преобразователь биометрия-код на базе корреляционных нейронов дает гораздо меньший процент ошибок и в разы большую длину ключа, чем классическая модель на базе алгоритма обучения ГОСТ Р 52633.5. Количество ошибок составило 3,26 %. При изменении состояния субъекта (опьянении или сонном состоянии) для разработанного метода количество ошибок повышается не столь существенно, чем для классической модели нейросетевого преобразователя биометрия-код.* ***Практическая значимость:*** *результаты могут использоваться для повышения защищенности компьютерных ресурсов от неавторизованного доступа и биометрических данных от компрометации.* ***Обсуждение:*** *объединение нейронов различного типа в единый слой позволит создать более устойчивые и надежные нейросетевые преобразователи биометрия-код.*

Ключевые слова *— защищенное исполнение нейросетевых алгоритмов, обработка коррелированных биометрических признаков, голосовая биометрия, нейросетевые преобразователи биометрия-код, анализ временных рядов, автокодировщики.*

Для цитирования: Сулавко А. Е., Иниватов Д. П., Васильев В. И., Ложников П. С. Аутентификация по голосовым паролям с обеспечением конфиденциальности биометрических данных на основе корреляционных нейронов. *Информационно-управляющие системы*, 2024, № 2, с. 21–38. doi:10.31799/1684-8853-2024-2-21-38, EDN: YIVAYM
For citation: Sulavko A. E., Inivatov D. P., Vasilyev V. I., Lozhnikov P. S. Authentication based on voice passwords with the biometric template protection using correlation neurons. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 21–38 (In Russian). doi:10.31799/1684-8853-2024-2-21-38, EDN: YIVAYM

Введение

Сегодня мировой рынок биометрии проходит фазу активного роста (по данным MarketsandMarkets, к 2025 г. его объем составит 68 млрд долл.). Биометрические системы внедряются повсеместно: на объектах критической информационной инфраструктуры, в банковской сфере, государственном секторе (более 80 стран используют биометрические паспорта), в сфере управления транспортом и городом. Рост рынка биометрических систем обусловлен новыми тенденциями и вызовами, с которыми столкнулись общество и государство:

— увеличением объемов данных о действиях пользователей в сети Интернет, которые могут быть использованы в злоумышленных целях (обострились проблемы приватности, анонимности пользователей и защищенности биометрических шаблонов от компрометации);

— применением технологий искусственного интеллекта (ИИ) для реализации хакерских атак, дезинформации, мошенничества, фальсификации биометрических образов человека (например, при помощи deepfake, голосовых синтезаторов);

— заменой традиционных биометрических образов отпечатка пальца на более удобные образы голоса, лица и др., пригодные для бесконтактной аутентификации, но в большей степени подверженные дрейфу (изменчивости).

В связи с этим современная высоконадежная биометрическая система должна строиться на основе доверенного ИИ, устойчивого к деструктивным факторам (дрейфу биометрических данных, компьютерным атакам). В России системы вы-

соконадежной биометрической аутентификации строятся на базе специальных архитектур ИИ — нейросетевых преобразователей биометрия-код (НПБК), которые позволяют связать биометрический образ субъекта с его криптографическим ключом или паролем [1].

Одной из перспективных биометрических модальностей является голос. Данный тип образов вместе с изображением лица используется в единой биометрической системе в соответствии с Федеральным законом № 572. Однако голосовые образы уязвимы с точки зрения компрометации, поэтому в ответственных приложениях лучше использовать не открытый голосовой образ (как при текстонезависимом распознавании диктора), а тайный образ — пароль, который произносится при аутентификации.

Настоящее исследование посвящено разработке метода биометрической аутентификации по голосу с обеспечением защищенности данных голоса от компрометации и устойчивости к их дрейфу. Работа является продолжением исследований [1], так как за основу предлагаемого метода взята модель НПБК на базе корреляционных нейронов (анализирующих корреляцию между признаками), которая изначально была предложена для аутентификации по внутреннему строению уха.

Краткий анализ проблемы и достигнутых результатов

В мировой практике сложилось несколько подходов к повышению надежности биометрических систем аутентификации с обеспечением конфиденциальности биометрических данных, которые основаны на использовании нечетких экстракторов, отменяемой биометрии, искусственных нейронных сетей или шифровании, в том числе гомоморфном. Проблемы гомоморфного шифрования заключаются в склонности гомоморфных шифров к накоплению ошибок (чем больше математических операций произведено с гомоморфным шифртекстом, тем больше вероятность некорректного результата этих операций [2], а также низкой производительности. В подтверждение этому факту приведем несколько работ. В исследовании [3] применяются полное гомоморфное шифрование биометрических образов и параллельные вычисления. Авторы отмечают, что процедура распознавания личности обладает низким быстродействием. Разработана [4] модель защиты мультимодальных биометрических шаблонов на базе гомоморфного шифрования по стандарту ISO/IEC 24745:2011. Основной недостаток модели также заключается в низкой скорости. В работе [5] предлагается протокол аутентификации на основе радужки с использованием гомоморфного шифрования. Среди недостатков разработанного решения можно отметить низкую производительность.

Отменяемая биометрия позволяет хранить не исходные образы субъектов, а их шаблоны, искаженные при помощи необратимых функций. Восстановить изначальные образы из сохраненного шаблона не представляется возможным. В исследовании [6] реализован облачный сервис, в котором биометрические шаблоны защищены методом случайных проекций (точность биометрической аутентификации по параметрам радужки составила 99,55 %). В статье [7] авторы достигли коэффициента равной вероятности ошибок EER = 0,2 % (Equal Error Rate), представив систему аутентификации по лицу и отпечатку пальца с шифрованием шаблонов, основанную на применении эволюционного генетического алгоритма.

Работа нечетких экстракторов (fuzzy vault, fuzzy extractor, fuzzy commitment, fuzzy embedder) обусловлена слабыми решающими правилами — неспособностью анализировать данные подобно нейронным сетям, и в случае с недостаточно информативными признаками экстракторы демонстрируют относительно низкую эффективность в задаче обработки рукописных образов (доля ошибок «ложного допуска» FAR = 0,2 % (False Acceptance Rate) при доле ошибок «ложного отказа» FRR = 76,53 % (False Rejection Rate), а также FAR = 6,91 % при FRR = 7,85 %) [8]. Применение схемы fuzzy vault к векторам извлеченных из изображений лиц с использованием методов квантования и бинаризации признаков исследуется в работе [9]. Ученые достигли показателей FAR = 1 % при FRR = 0,1 %.

На данный момент действует ряд международных стандартов, связанных с вопросами защиты биометрических систем от компьютерных атак (ISO/IEC 19792:2009, ISO/IEC 24761:2019, ISO/IEC 24745:2022, ISO/IEC 30107). Но эти стандарты не позволяют устранить ряд актуальных угроз (извлечение знаний моделей ИИ, компрометацию открытых биометрических образов, состязательные атаки). В России действует серия национальных ГОСТ Р 52633, не имеющих международных аналогов. Эти ГОСТы регламентируют особенности разработки, обучения и тестирования систем высоконадежной биометрической аутентификации, которые должны строиться на базе НПБК, позволяющих связать криптографический ключ или пароль пользователя с его биометрическим образом. НПБК не имеют недостатков, характерных для нечетких экстракторов [10], и значительно их превосходят, так как дают большую длину ключа при

меньших значениях FRR и FAR [11]. Технически НПБК позволяют связать биометрический образ с ключом любой длины. Однако определенные ограничения все-таки существуют.

Первое из них не позволяет использовать каждый биометрический признак дважды при нейросетевой обработке (входы нейронов в НПБК не могут дублироваться), иначе НПБК становятся подверженными атаке Маршалко [12], основанной на наблюдении одинаковых весовых коэффициентов в таблицах нейросетевых функционалов. С учетом этого требования длина ключа для НПБК будет снижена. Например, для технологии аутентификации в защищенном режиме по рукописной подписи при наличии 416 признаков, извлекаемых из рукописных образов, может получиться 26 нейронов, у которых имеется по 16 неповторяющихся входов [13]. Длина ключа 26 бит явно недостаточна для практических целей. Аналогично дело обстоит и с голосовыми образами (при том же количестве входов с учетом соблюдения данного требования при количестве признаков от 521 до 728 [14] мы получим длину ключа от 32 до 49 бит).

Второе ограничение связано с возможностью проведения атаки «извлечения знаний» из обученного НПБК путем статистического анализа стабильности выходов ПБК при поступлении на его входы естественных и синтетических образов «Чужих». В работах [10, 11] описываются результаты исследования НПБК, в том числе касающиеся энтропии их откликов при поступлении на вход образов «Чужих». Для защиты от атаки «извлечения знаний» можно применить действенный метод криптографической защиты. Нейроны выстраиваются в цепочку, и после обучения НПБК параметры каждого нейрона шифруются на ключе, зависящем от выходов всех предыдущих нейронов в цепочке [10, 11]. Тем не менее известны другие варианты атак на классические НПБК [15], которые могут работать даже при реализации криптографической защиты. Атакам подвержены нейроны с бинарными выходами (когда каждый нейрон на выходе дает один бит), которые являются «узким местом».

Наконец, одной из ключевых проблем машинного обучения и классических НПБК в частности является проблема концептуального дрейфа — изменения взаимосвязи между данными и прогнозируемым явлением, которое не было учтено при обучении модели ИИ. Если дрейф данных (сбои датчиков, изменение единиц измерения) часто устраняется относительно легко (следует продумать все возможные изменения, которые могут быть спрогнозированы при обучении модели), то концептуальный дрейф устранить затруднительно, так как нельзя заранее знать, как в будущем изменится прогнозируемое явление.

В биометрии дрейф модели можно условно разделить на две категории:

— кратковременный (голос меняется при опьянении субъекта или заболевании горла) [16];

— долговременный (медленные и, как правило, необратимые со временем изменения биометрического образа пользователя).

Несмотря на различные причины дрейфа, оба типа изменений крайне сложно спрогнозировать. Если для статических биометрических образов (отпечатка пальца, радужки, сетчатки, лица) дрейф появляется только при физических нарушениях, таких как травма, порезы и т. д., то для динамических биометрических образов этих изменений почти невозможно избежать (например, голос меняется в зависимости от эмоционального состояния).

Можно сформулировать несколько общих приемов и подходов, предназначенных для снижения негативного влияния дрейфа. Например, периодическое обновление модели дает положительный эффект, если есть данные для переобучения. При этом может применяться взвешивание данных — присвоение большего веса наиболее актуальным обучающим примерам и меньшего веса данным, полученным давно. Для своевременного обнаружения дрейфа используются метрики, вычисляющие статистические характеристики данных с учетом ретроспективы [17, 18], а также ансамблевые методы классификации. Однако эти методы дают ограниченный эффект. Наиболее эффективным подходом является онлайн-обучение (обучение или дообучение в процессе функционирования), которое позволяет снизить влияние концептуального дрейфа. Однако классический НПБК не может работать в режиме онлайн-обучения (весовые коэффициенты НПБК не могут быть скорректированы путем извлечения из них и устранения информации, потерявшей актуальность).

В настоящем исследовании мы пошли иным путем, используя модель нейрона, которая сама по себе, как оказалось, обладает некоторой устойчивостью к дрейфу голосовых данных.

Наборы голосовых данных для проведения экспериментов

Существующие наборы данных, которые возможно использовать для тестирования методов биометрической голосовой аутентификации, не учитывают психоэмоционального состояния диктора (VoxCeleb, TIMIT, RedDots, Common Voice, VoxForge, LibriSpeech, NIST SRE). Кроме того, большая часть этих наборов данных применима для систем текстонезависимого распозна-

вания личности диктора. Наиболее актуальной на сегодня базой голосовых паролей, используемой для оценки современных методов текстозависимой классификации дикторов, является RedDots [19]. Набор данных включает голоса 100 испытуемых, речь которых записывалась еженедельно в течение года. Каждый доброволец произносил 24 предложения на каждой сессии, включая 22 повторяющихся и два свободных текстовых. Всего в наборе данных 124 800 записей. Корпус создан для исследования влияния феномена «старения» на распознавание голоса. Данная база использовалась в настоящем исследовании для тестирования предлагаемой модели.

Психоэмоциональное (психофизиологическое) состояние субъекта является одним из ключевых факторов, вызывающих дрейф [16]. Поэтому был сформирован собственный набор данных, учитывающий следующие состояния испытуемых: нормальное (спокойное), возбужденное, сонное и алкогольного опьянения. Набор данных можно разделить на две части.

1. «Зарегистрированные субъекты» («Все Свои»): 65 дикторов, каждый воспроизвел образ определенного голосового пароля не менее 80 раз, данные собраны в три этапа с интервалом несколько недель:

— на 1-м этапе каждый испытуемый ввел не менее 40 примеров, при этом испытуемые пребывали в нормальном состоянии (выспались перед экспериментом и не подвергались никаким воздействиям);

— на 2-м этапе каждый испытуемый ввел 20 примеров в сонном состоянии после приема седативных средств;

— на 3-м этапе каждый испытуемый ввел 20 примеров в состоянии легкого алкогольного опьянения, при котором концентрация алкоголя в крови составляет от 0,5 до 1 ‰ (согласно рекомендациям Минздрава, в данном состоянии речь субъекта становится менее разборчивой), количество алкоголя для получения данной стадии опьянения рассчитывалось по формуле Видмарка исходя из пола и веса субъекта [16].

Примеры, полученные на этапе 1, могут целиком или частично использоваться для обучения системы, в том числе в составе валидационной выборки (в настоящей работе для обучения использовано по 20 примеров, остальные — для тестирования, валидационная выборка при обучении НПБК не применяется). Примеры, полученные на этапах 2 и 3, рекомендуется использовать только для тестирования.

2. «Неизвестные Чужие»: 650 примеров других голосовых образов (фраз, паролей), воспроизведенных другими субъектами, не вошедшими в базу «Зарегистрированные субъекты». Данная выборка должна использоваться только в целях тестирования.

Для записи использовался микрофон Fifine K680 (чувствительность 34 дБ, диапазон частот 20÷20 000 Гц, соотношение сигнал/шум 78 дБ). Запись производилась в тихом помещении при отсутствии внешних источников шума.

Звуковые сигналы имеют следующие параметры: размер семпла $\Psi = 16$ бит, частота дискретизации $\Omega = 16$ кГц. Сформированный набор данных применялся для обучения и тестирования НПБК. Открытые наборы данных VoxCeleb и TIMIT использовались для предварительного обучения нейронных сетей, извлекающих признаки из голосового образа перед подачей образа в НПБК.

Архитектурные принципы построения метода аутентификации субъектов по голосу на базе НПБК

Для реализации концепции защищенного исполнения нейросетевых алгоритмов ИИ в задачах классификации образов предлагается разделить функционал ИИ на блок выделения признаков и НПБК. Блок извлечения признаков преобразует образ в вектор фиксированной длины (эту операцию можно назвать ортогонализацией образа). На этапе извлечения признаков образ нормируется, и из него удаляется незначимая информация. Блок извлечения признаков может быть реализован на основе практически любых подходов (нейронных сетей, классических методов спектрального и корреляционного анализа и др.). В общем случае блок извлечения признаков является зависимым от предметной области, так как для разных приложений входные данные могут кардинально отличаться, как и характер извлекаемой из образа информации (вектора признаков). Для обработки звука часто используются методы x-vector, d-vector, i-vector, быстрое преобразование Фурье, вычисление мел-кепстральных коэффициентов или вейвлет-преобразование. Разные подходы могут комбинироваться. В настоящей работе блок извлечения признаков строится на базе автокодировщиков.

Обучение автокодировщика [20] гипотетически может вестись алгоритмом градиентного спуска или его модификациями. Для синтеза и обучения НПБК в автоматическом режиме требуется отдельный робастной алгоритм.

Вектор признаков, извлеченный автокодировщиками, поступает на вход НПБК. Обучение НПБК должно быть автоматическим и робастным.

Извлечение признаков

Предобработка данных голосовых образов

Прежде всего голосовые образы были преобразованы в спектрограммы. Чтобы выделить из акустических образов полезную информацию и снизить дисперсию случайных выбросов при разложении сигнала в ряды Фурье, спектрограммы были преобразованы в усредненный по всем окнам (по всем временным промежуткам) амплитудный спектр (путем интегрирования спектрограмм). В настоящем исследовании использовались следующие параметры быстрого оконного преобразования Фурье: размер окна W_{size} = 4096 (четверть секунды), шаг W_{step} = 256. Длина усредненного спектра 2048 амплитуд.

Архитектуры автокодировщиков и их обучение

В голосовой биометрии часто используются методы извлечения так называемых мелкепстральных коэффициентов, а также x-, d- и i-векторов. Весомая часть исследований посвящена сравнению данных методов, что привело к выводу, что i-vector позволяет создавать менее ресурсоемкие системы, в то время как x-vector обеспечивает более высокую эффективность благодаря глубокому анализу: 5,71 % против 9,23 % EER при использовании вероятностного линейного дискриминантного анализа в качестве классификатора [21].

Альтернативным направлением является применение автокодировщиков. Можно применить сразу несколько схожих архитектур, обученных на одних и тех же данных, что позволит получить множество признаков с сильной взаимной корреляцией, необходимых для построения НПБК на базе корреляционных нейронов. По этой причине для извлечения признаков решено использовать две схожие архитектуры автокодировщиков (рис. 1). Ожидаемо, что признаки, извлекаемые автокодировщиками со схожими архитектурами, обученными на одной и той же выборке, будут в большей степени коррелированы.

При обучении применялся подход из работы [1]. Мы взяли речевые сигналы из наборов данных TIMIT и VoxCeleb1 (наборы данных имеют одинаковые параметры голосовых сигналов Ψ = 16 бит, Ω = 16 кГц [22]) с длительностью, соответствующей короткому голосовому паролю. Далее была выполнена аугментация данных [23] — образы преобразовывались в четыре представления, каждое из которых — это усредненный спектр, полученный при помощи одного из четырех типов окон (прямоугольного, Блэкмана, Барлетта, Хэмминга). Общее количество образов превысило 285 000 после аугментации. Автокодировщики обучены оптимизатором Adam (20 эпох).

При извлечении признаков также использованы две вариации образа — на базе прямоугольной оконной функции Фурье и оконной функции Хэмминга. Этот прием также применялся для получения большего числа сильно коррелированных признаков. Ожидаемо, что усредненные спектры, полученные с использованием различных типов окон, после обработки кодировщиком дадут коррелированные векторы признаков, но все-таки имеющие отличия. Чем больше коррелированных пар признаков, тем выше эффективность НПБК на базе корреляционных нейронов [1].

Математические основы используемой модели НПБК

Искривление пространства признаков

Для расчета расстояния в искривленном пространстве признаков может применяться мера Минковского

$$y = \sqrt[g]{\sum_{j=1}^{n}\left|\frac{(m_j - a_j)}{\sigma_j}\right|^g},$$

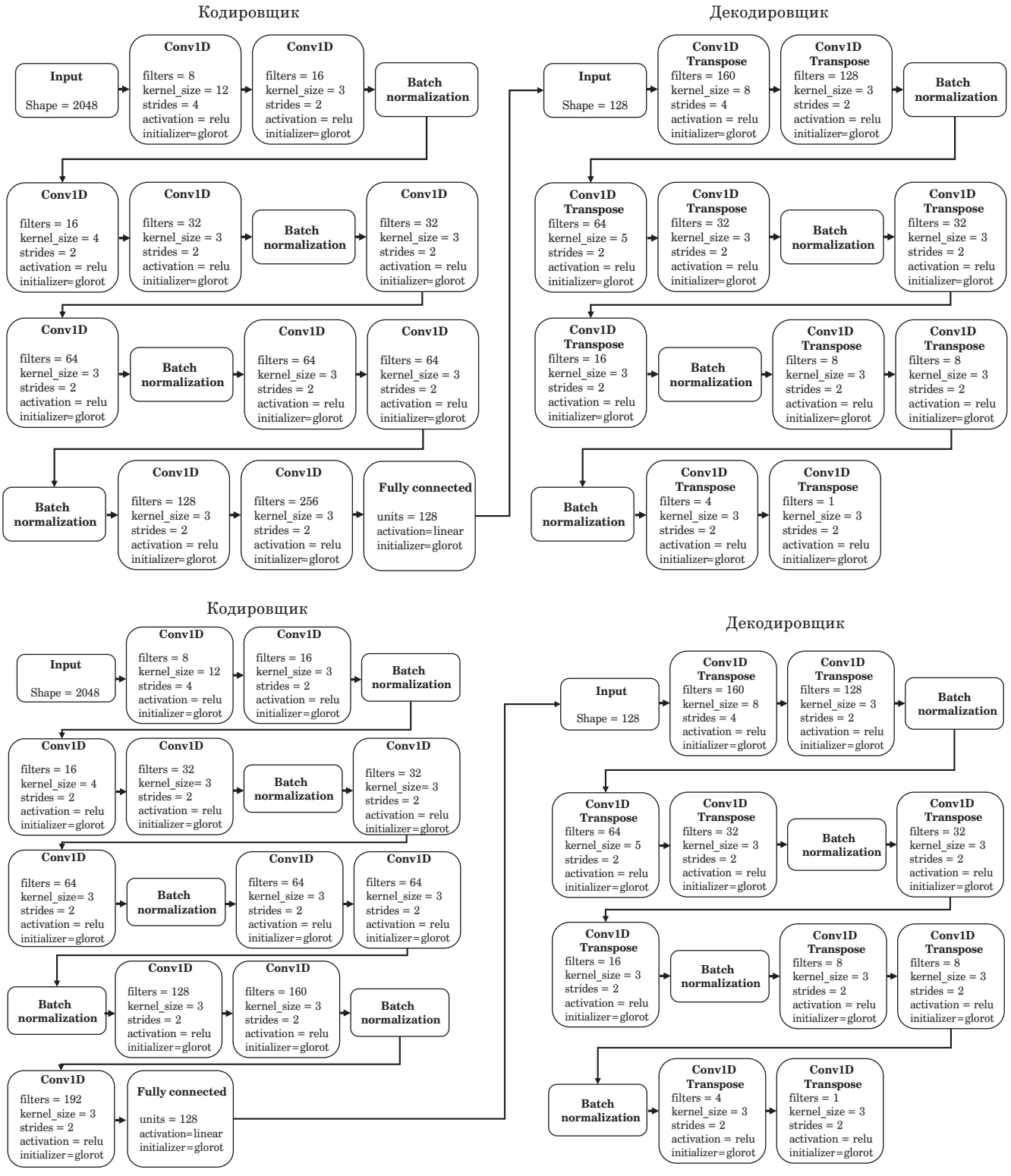
где g — степенной коэффициент; n — число признаков; m_j и σ_j — математическое ожидание и стандартное отклонение j-го признака для класса «Свой» (класс зарегистрированного пользователя); a_j — значение j-го признака.

Искривление признакового пространства возникает из-за корреляции между признаками (рис. 2). Относительно различных классов пространство признаков искривлено по-разному, так как биометрический образ каждого человека имеет уникальную матрицу коэффициентов корреляции

$$C_{j,t} = \frac{\sum_{k=1}^{K_G}(a_{t,k} - m_t)(a_{j,k} - m_j)}{\sqrt{\sum_{k=1}^{K_G}(a_{t,k} - m_t)^2 \sum_{k=1}^{K_G}(a_{j,k} - m_j)^2}}, \quad (1)$$

где K_G — количество обучающих примеров образа «Свой» (далее K_I — количество обучающих примеров образа «Чужие»); k — порядковый номер примера в обучающей выборке. На рис. 2 для класса 2 расстояние «*а*» на самом деле должно быть больше, чем расстояние «*б*», так как пространство признаков является не плоским, а искривленным.

Важным показателем j-го признака также является уровень его информативности, который

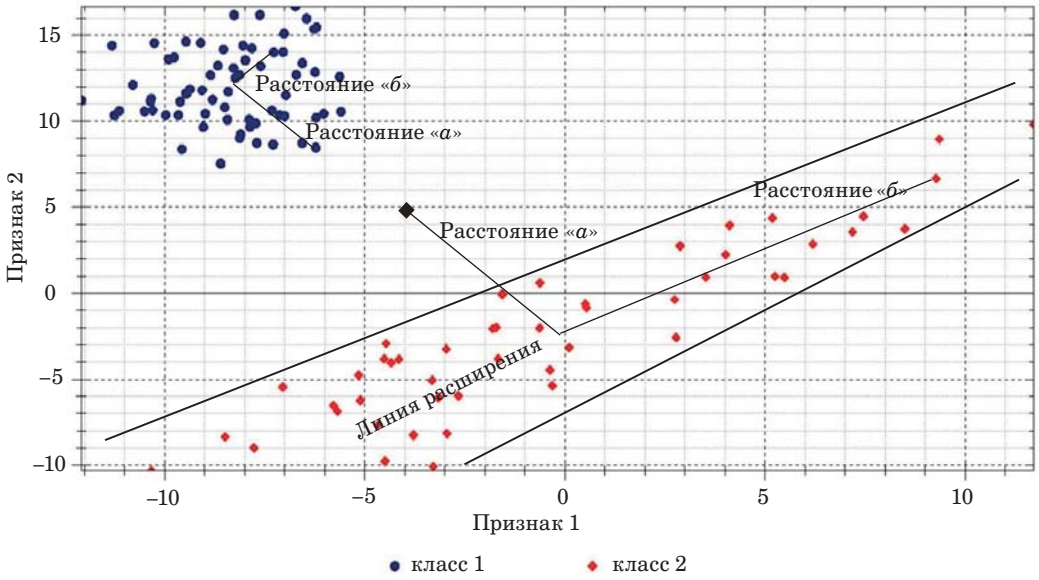


■ ***Рис. 1.*** Архитектуры использованных автокодировщиков
■ ***Fig. 1.*** Architectures of the used autoencoders

определяется количеством собственной информации для определенного класса образов [1]:

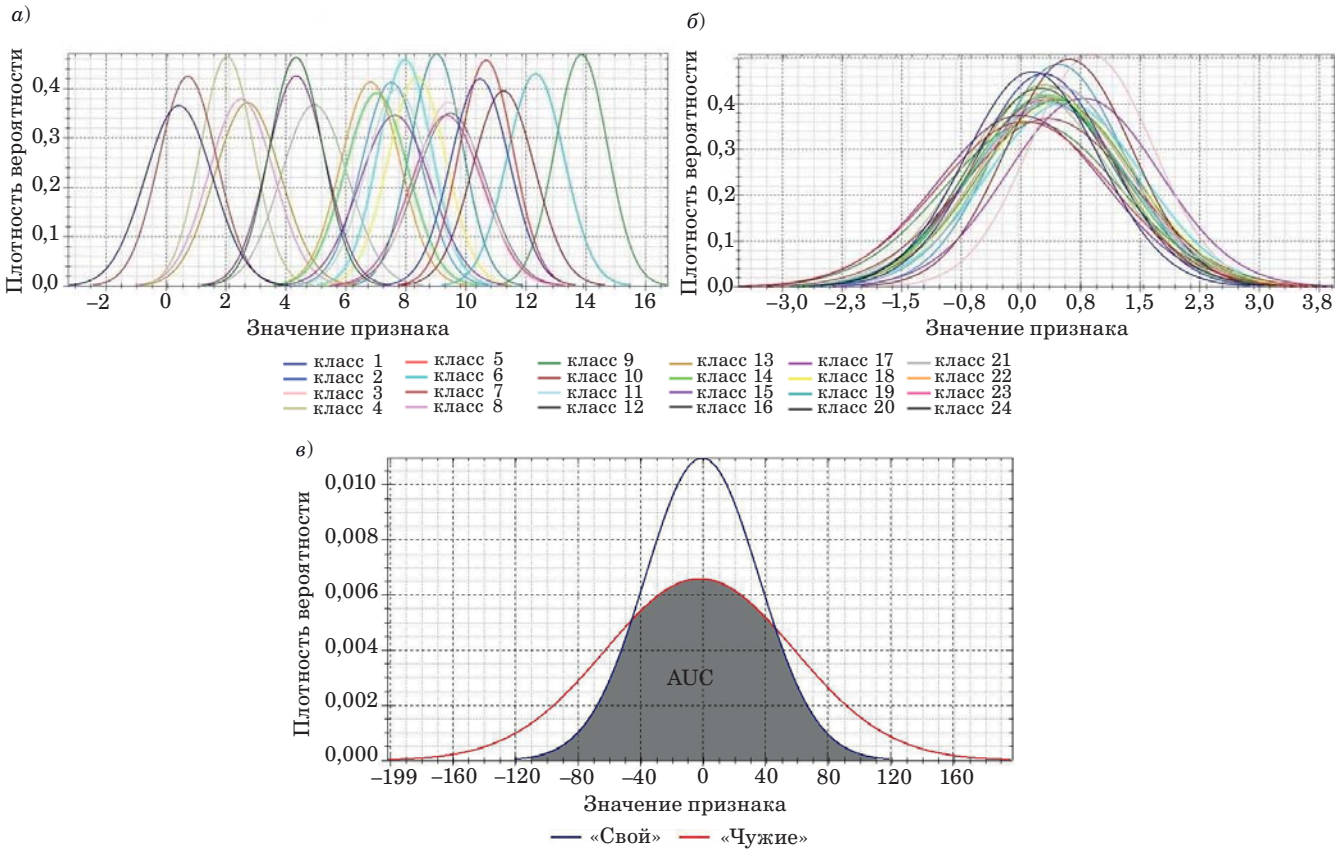
$$I_j = -\log_2(AUC(\Phi_G(a_j), \Phi_I(a_j))), \qquad (2)$$

где AUC – площадь, ограниченная функциями плотности вероятности (ФПВ) «Свой» $\Phi_G(a_j)$ и «Чужие» $\Phi_I(a_j)$, а также осью абсцисс (рис. 3, *а–в*). $\Phi_G(a_j)$ характеризует значения при-



■ ***Рис. 2.*** Пространство признаков является «плоским» относительно класса 1 (признаки независимы) и искривленным относительно класса 2 (признаки положительно коррелированы), черная точка — это образ «Чужого»

■ ***Fig. 2.*** The feature space is “flat” relative to class 1 (features are independent) and curved relative to class 2 (features are positively correlated), the black dot is the “Imposter” image



■ ***Рис. 3.*** Примеры ФПВ признака: *а*, *б* — 24 классов «Свой» ($I_{bit} \approx 1{,}75$; $I_{bit} \approx 0{,}15$ соответственно); *в* — расчет AUC через построение ФПВ «Свой» и «Чужие» [1]

■ ***Fig. 3.*** Examples of the probability density function of a feature: *a*, *б* — 24 «Genuine» classes ($I_{bit} \approx 1{,}75$; $I_{bit} \approx 0{,}15$ respectively); *в* — calculating AUC by constructing the probability density function «Genuine» and «Imposters» [1]

знака для определенного субъекта, $\Phi_I(a_j)$ характеризует значения этого же признака для всех субъектов в целом [1].

Изменяя параметр g, можно добиться снижения количества ошибок классификации. Чтобы это продемонстрировать, в настоящем исследовании проведен вычислительный эксперимент по распознаванию образов в пространстве 200 абстрактных (имитированных) признаков. Все признаки имели нормальное распределение значений (наиболее распространенный случай для биометрии). На каждом этапе эксперимента генерировалось два пространства признаков — независимых ($C \approx 0$) и зависимых ($C > 0$). Отличия этапов заключались в информативности и уровне коррелированности зависимых признаков (см. рис. 3): $I \approx 0{,}15$ при $C \approx 0$; $I \approx 0{,}15$ при $C \approx 0{,}9$; $I \approx 1{,}75$ при $C \approx 0{,}1$; $I \approx 1{,}75$ при $C \approx 0$.

Генерируемые классы образов отличались между собой параметрами распределения признаков. Значения независимых признаков генерировались методом Монте-Карло под соответствующие параметры классов. Для классов с зависимыми признаками перед формированием соответствующих образов $\bar{a}$ значения каждого признака внутри класса были отсортированы по возрастанию. Таким образом, в эксперименте смоделировано четыре варианта пространства признаков (зависимых и коррелированных с учетом двух уровней информативности). Для каждого случая сгенерировано 500 классов по 125 примеров образа на класс. Каждый классификатор обучался на 25 случайных сгенерированных примерах, остальные 100 примеров использовались для тестирования. Исходя из порогового значения для меры Минковского, принималось решение об отнесении данных к категории «Свой» или «Чужие». По окончании сессии рассчитывался показатель EER. Обобщенные результаты эксперимента показаны на рис. 4, *а–в* (все вероятности ошибок представлены в логарифмической шкале).

Мера Минковского позволяет точнее определять расстояния в искривленном пространстве признаков, что дает хорошие результаты, только если корреляционная зависимость между признаками примерно одинакова и не является очень высокой, т. е. признаки следует группировать. Однако при сильном искривлении пространства признаков количество ошибочных решений остается слишком большим (см. рис. 4, *в*). На практике корреляционная зависимость между признаками различна.

Мера близости и мета-признаки Байеса — Минковского

Корреляция не только искривляет пространство признаков, но и несет в себе дополнительную информацию об образах, которая «переносится» в «скрытые» измерения. Чтобы извлечь данную информацию, предложена мера Байеса — Минковского [1]

$$y = \sqrt[g]{\sum_{j=1}^{n} \left| \left| \frac{(m_t - a_t)}{\sigma_t} \right|^g - \left| \frac{(m_j - a_j)}{\sigma_j} \right|^g \right|}, j \neq t. \qquad (3)$$

Эта метрика принимает тем меньшие значения, чем выше $C_{j,t}$.

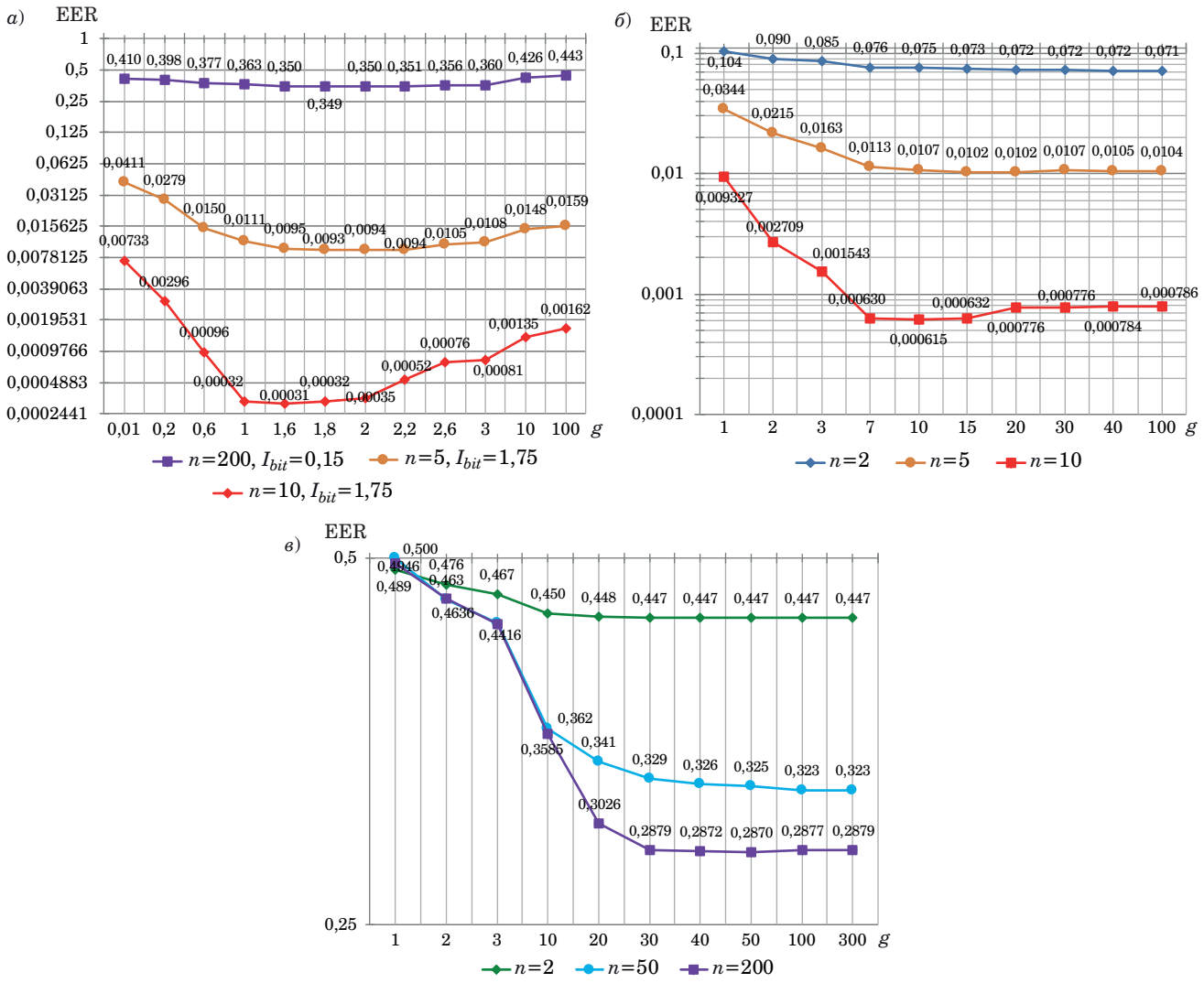
Собственная информация, которая содержится в признаках и рассчитывается по формуле (2), и та, что содержится в их корреляционных связях, различны. Чтобы показать это, в данной работе проведен еще один эксперимент по распознаванию образов мерой Байеса — Минковского (3) с условиями, аналогичными предыдущему эксперименту. Из представленных данных (рис. 5, *а–г*) видно, что оптимум g для меры (3) меняется в каждом рассмотренном случае. Если признаки независимы, то минимум по EER достигается при $g > 1$, если существенно коррелированы — при $0{,}7 \le g \le 1$.

Динамика изменения EER для меры Байеса — Минковского имеет обратную тенденцию по сравнению с показателями EER для меры Минковского. Если признаки коррелированы, мера Байеса — Минковского дает в разы более высокий результат, чем при независимых признаках. Причем вероятность ошибок распознавания в пространстве сильно коррелированных ($C \approx 0{,}9$) признаков для меры Байеса — Минковского ниже (см. рис. 5, *в*), чем уровень ошибок для меры Минковского в случае независимости признаков (см. рис. 4, *а*) при той же информативности и количестве признаков ($I_{bit} \approx 0{,}15$ и $n = 200$).

Таким образом, мера Байеса — Минковского является «антагонистом» по отношению к мере Минковского, так как обладает противоположными свойствами. Кроме того, мы видим, что информативность I_{bit} влияет на результат, как и корреляция C, и это влияние не взаимоисключающее (информативные признаки дают более хороший результат, чем малоинформативные, даже при отсутствии корреляции, но при ее наличии результат еще лучше). Соответственно, *информация о различии классов образов, которая содержится в признаках и их корреляционных связях, не дублируется*.

Под мета-признаком далее понимается выражение

$$a'_\iota = a'_{t,j} = f(a_t, a_j) = \left| a_t - a_j \right|,$$
$$j > t, \iota = \sum_{i=1}^{t-1} (n - i) + j - t. \qquad (4)$$



■ ***Рис. 4.*** Влияние g и n на EER (мера Минковского): *а* — признаки независимы ($C = 0$), различная информативность; *б* — признаки информативны ($I_{bit} \approx 1{,}75$), слабо зависимы ($C \approx 0{,}1$); *в* — признаки малоинформативны ($I_{bit} \approx 0{,}15$), сильно зависимы ($C \approx 0{,}9$)

■ ***Fig. 4.*** Effect of g and n on EER (Minkowski measure): *а* — the features are independent ($C = 0$), different information content; *б* — the features are informative ($I_{bit} \approx 1.75$), weakly dependent ($C \approx 0.1$); *в* — the features are little informative ($I_{bit} \approx 0.15$), highly dependent ($C \approx 0.9$)

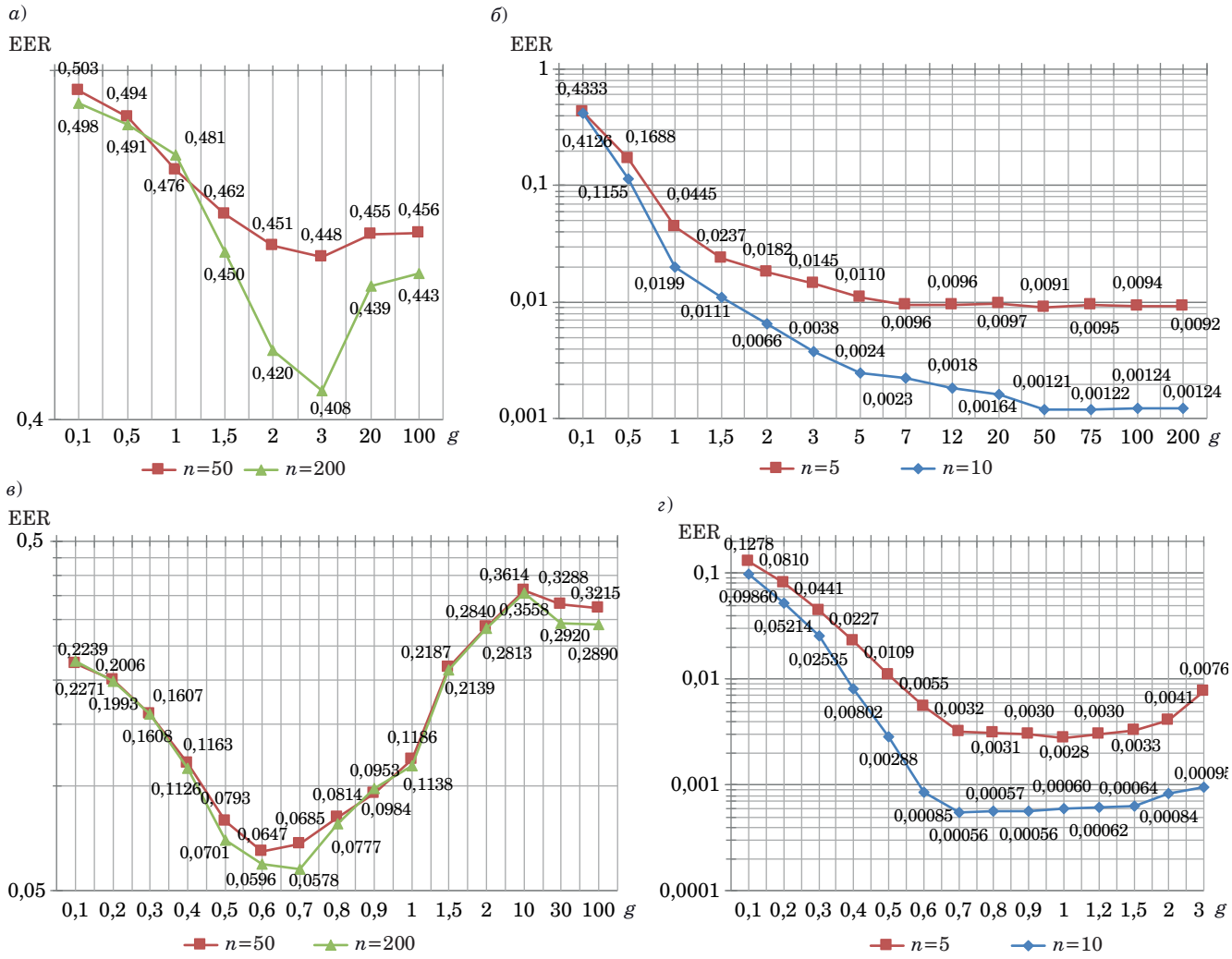
Чем меньше $|a'_{j,t}|$, тем выше внутриклассовая корреляция между признаками j и t, если $C_{j,t} = 1$, то $a'_{t,j} \approx 0$ при условии, что области значений признаков нормированы и центрированы. Размерность пространства мета-признаков Байеса — Минковского составляет

$$n' = 0{,}5(n(n-1)) = 0{,}5n^2 - 0{,}5n.$$

Мера Байеса — Минковского (3) — это линейный классификатор в пространстве мета-признаков, подобных (4), но нормирующих и центрирующих их значения относительно образов «Свой» с учетом априорных знаний параметров m_j и σ_j. Проблема метрики (3) в том, что параметры m_j и σ_j компрометируют информацию о классе образов «Свой». Без этих параметров мера близости на первый взгляд обладает меньшей информацией, однако не все так однозначно. Классификация образов возможна и без знаний m_j и σ_j.

Модель корреляционного нейрона и алгоритм обучения НПБК

Пусть корреляционный нейрон соединяется с мета-признаками (4), которые были порождены парами признаков с сильной взаимной корреляцией. Один мета-признак может быть связан только с одним корреляционным нейроном во избежание реализации атак, основанных на поиске общих связей нейронов [12, 15]. Введем два уровня коррелированности признаков: $C_{\_} = -0{,}5 > C_{j,t}$



■ ***Рис. 5.*** Влияние g и n на EER (мера Байеса — Минковского): *а* — признаки независимы (C=0) и малоинформативны ($I_{bit} \approx 0{,}15$); *б* — признаки независимы (C=0) и весьма информативны ($I_{bit} \approx 1{,}75$); *в* — признаки сильно коррелированы (C=0,9) и малоинформативны ($I_{bit} \approx 0{,}15$); *г* — признаки слабо коррелированы (C=0,1) и информативны ($I_{bit} \approx 1{,}75$)

■ ***Fig. 5.*** Effect of g and n on EER (Bayes — Minkowski measure): *а* — the features are independent (C=0) and uninformative ($I_{bit} \approx 0.15$); *б* — the features are independent (C=0) and very informative ($I_{bit} \approx 1.75$); *в* — the features are highly correlated (C=0.9) and uninformative ($I_{bit} \approx 0.15$); *г* — the features are weakly correlated (C=0.1) and informative ($I_{bit} \approx 1.75$)

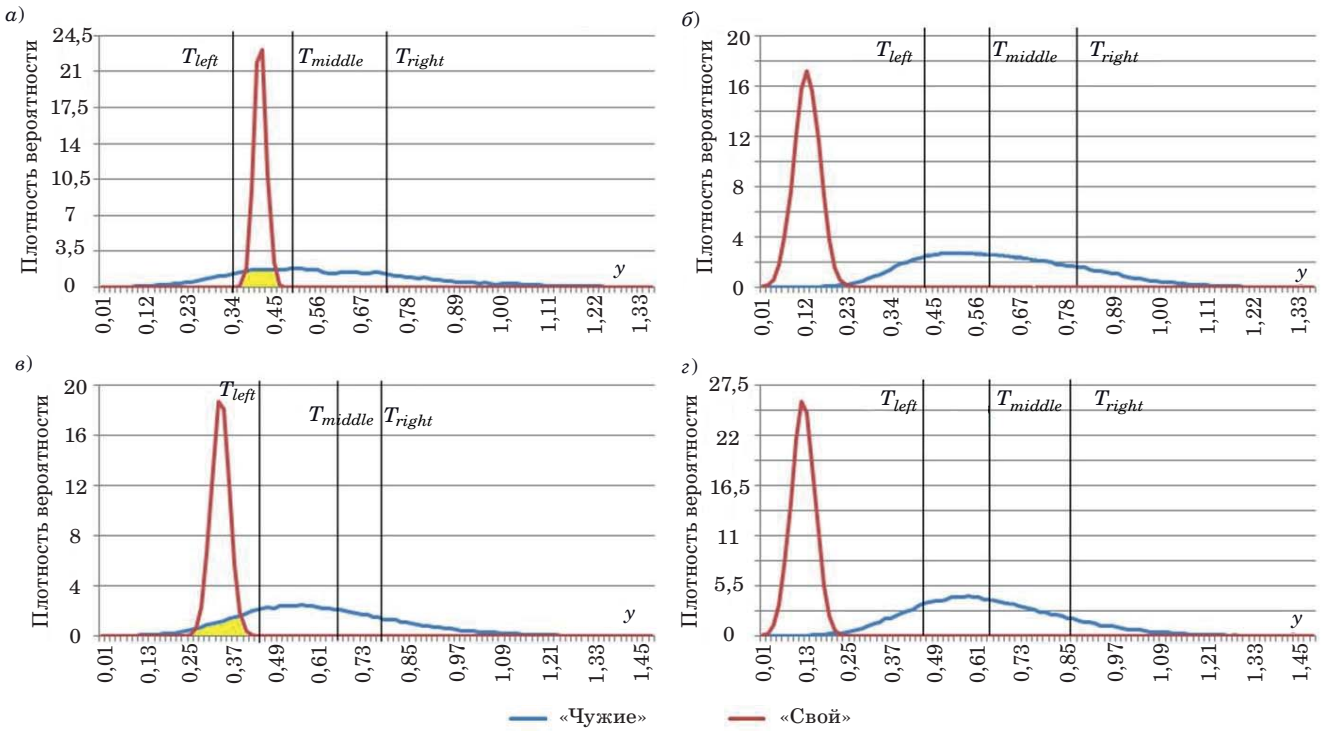
и $C_+ = 0{,}5 < C_{j,t}$. Корреляционный нейрон не должен быть связан с признаками, которые имеют уровень взаимной коррелированности $|C_{-+}| < 0{,}3$. Нейрон строится на базе метрики взвешенного среднеквадратичного отклонения (5) значений мета-признаков (4), которая позволяет отделить как положительно коррелированные, так и отрицательно коррелированные данные (рис. 6). Это происходит потому, что при наличии сильной положительной или отрицательной корреляции между исходными признаками выражение $|a'_\iota - m'|$ имеет тенденцию давать более низкие значения:

$$y = \sqrt{\frac{1}{\eta}\sum_{\iota=1}^{n'} w_\iota \left(a'_\iota - m'\right)^2}, \qquad (5)$$

$$m' = \frac{\sum_{\iota^*=1}^{\eta} a'_{\iota^*}}{\eta},$$

где η — количество входов нейрона; w_ι — вес синапса под номером ι ($w_\iota \geq 0$; если $w_\iota = 0$, то ι-й мета-признак не соединяется с нейроном); ι^* — номер входа для сквозной нумерации (без учета входов, для которых $w_\iota = 0$). Вес синапса рассчитывается по формуле

$$w_\iota = \frac{\left|m''_{(G),\iota} - m''_{(I),\iota}\right|}{\sigma''_{(G),\iota} \cdot \sigma''_{(I),\iota}}, \qquad (6)$$



■ ***Рис. 6.*** Плотности вероятности значений меры (5) для сгенерированных данных после отображения (4) при $g = 1$, $I \approx 1{,}75$ бит: *а* — для всех классов $1 > C_{j,t} > 0{,}95$, $n' = 10$; *б* — для всех классов $-1 < C_{j,t} < -0{,}95$, $n' = 10$; *в* — для классов «Свой» $1 > C_{j,t} > 0{,}95$, для класса «Чужие» $|C_{j,t}| < 0{,}3$, $n' = 10$; *г* — для классов «Свой» $-1 < C_{j,t} < -0{,}95$, для класса «Чужие» $|C_{j,t}| < 0{,}3$, $n' = 10$

■ ***Fig. 6.*** Probability density graphs of the values of measure (5) for the generated data after display (4) with $g = 1$, $I \approx 1{,}75$ bits: *a* — for all classes $1 > C_{j,t} > 0{,}95$, $n' = 10$; *б* — for all classes $-1 < C_{j,t} < -0{,}95$, $n' = 10$; *в* — for the « Genuine» classes $1 > C_{j,t} > 0{,}95$, for the «Alien» class $|C_{j,t}| < 0{,}3$, $n'=10$; *г* — for the « Genuine» classes $-1 < C_{j,t} < -0{,}95$, for the «Alien» class $|C_{j,t}| < 0{,}3$, $n' = 10$

$$m''_{(G),\iota} = \frac{\sum_{k=1}^{K_G}\left(a''_{\iota,k} - m'\right)^2}{K_G},\quad m''_{(I),\iota} = \frac{\sum_{k=1}^{K_I}\left(a'_{\iota,k} - m'\right)^2}{K_I},$$

$$\sigma''_{(G),\iota} = \sqrt{\frac{\sum_{k=1}^{K_G}\left(\left(a'_{\iota,k} - m'\right)^2 - m''_{(G),\iota}\right)^2}{K_G}},$$

$$\sigma''_{(I),\iota} = \sqrt{\frac{\sum_{k=1}^{K_I}\left(\left(a'_{\iota,k} - m'\right)^2 - m''_{(I),\iota}\right)^2}{K_I}}.$$

После обучения нейрона параметры $m''_{(G),\iota}$, $m''_{(I),\iota}$, $\sigma''_{(G),\iota}$, $\sigma''_{(I),\iota}$ должны быть удалены.

Нейроны должны иметь четырехуровневую пороговую функцию активации

$$\phi(y) = \begin{cases} \text{"11"}, & y < T_{left} \\ \text{"10"}, & T_{left} \le y < T_{middle} \\ \text{"01"}, & T_{middle} \le y < T_{right} \\ \text{"00"}, & y \ge T_{right} \end{cases}, \qquad (7)$$

где T_{left}, T_{middle} и T_{right} — левый, средний и правый пороговые значения активации нейрона (см. рис. 6). В соответствии с предлагаемой моделью нейрон имеет четыре варианта активации {0, 1, 2, 3} и только один из них соответствует гипотезе «Свой», остальные соответствуют гипотезе «Чужие». О том, какое именно состояние активации соответствует гипотезе «Свой» (далее ϕ_G), известно только на этапе синтеза и обучения НПБК, злоумышленник не обладает этой информацией, так как она не сохраняется после настройки нейрона.

При поступлении образа «Свой» на выходе нейрона почти всегда должно возникать определенное состояние, а в других ситуациях состояния {0, 1, 2, 3} должны быть случайны. Поэтому для вычисления порогов необходимо рассчитать границы интервала значений откликов нейрона y на обучающие примеры «Свой» $[y_{G\,\min}, y_{G\,\max}]$ и «Чужие» $[y_{I\,\min}, y_{I\,\max}]$ по формуле

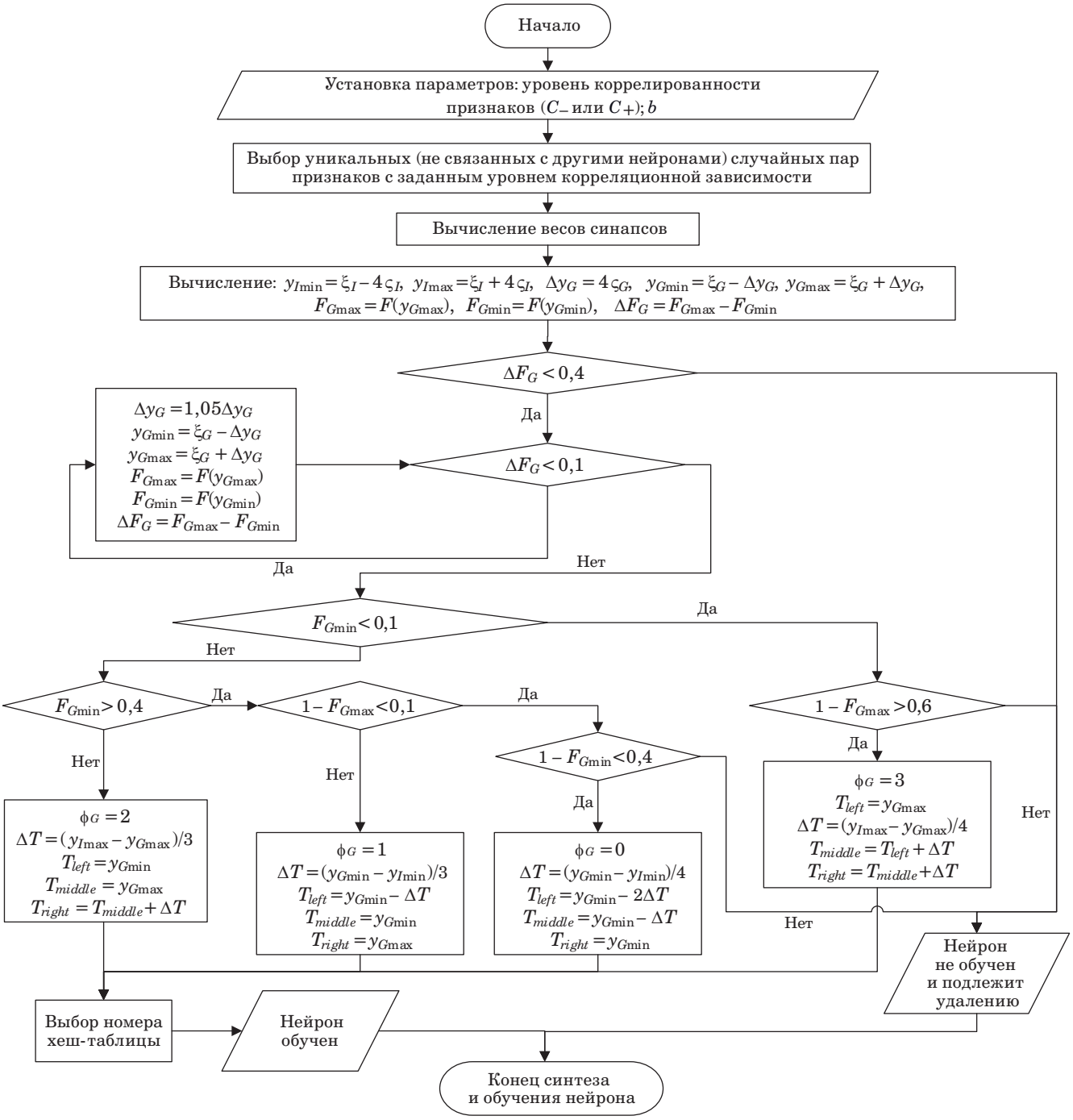
$$y_{\min} = \xi - 4\varsigma, y_{\max} = \xi + 4\varsigma \qquad (8)$$

и функции распределения нормального закона $F_G(y)$ и $F_I(y)$ [1]:

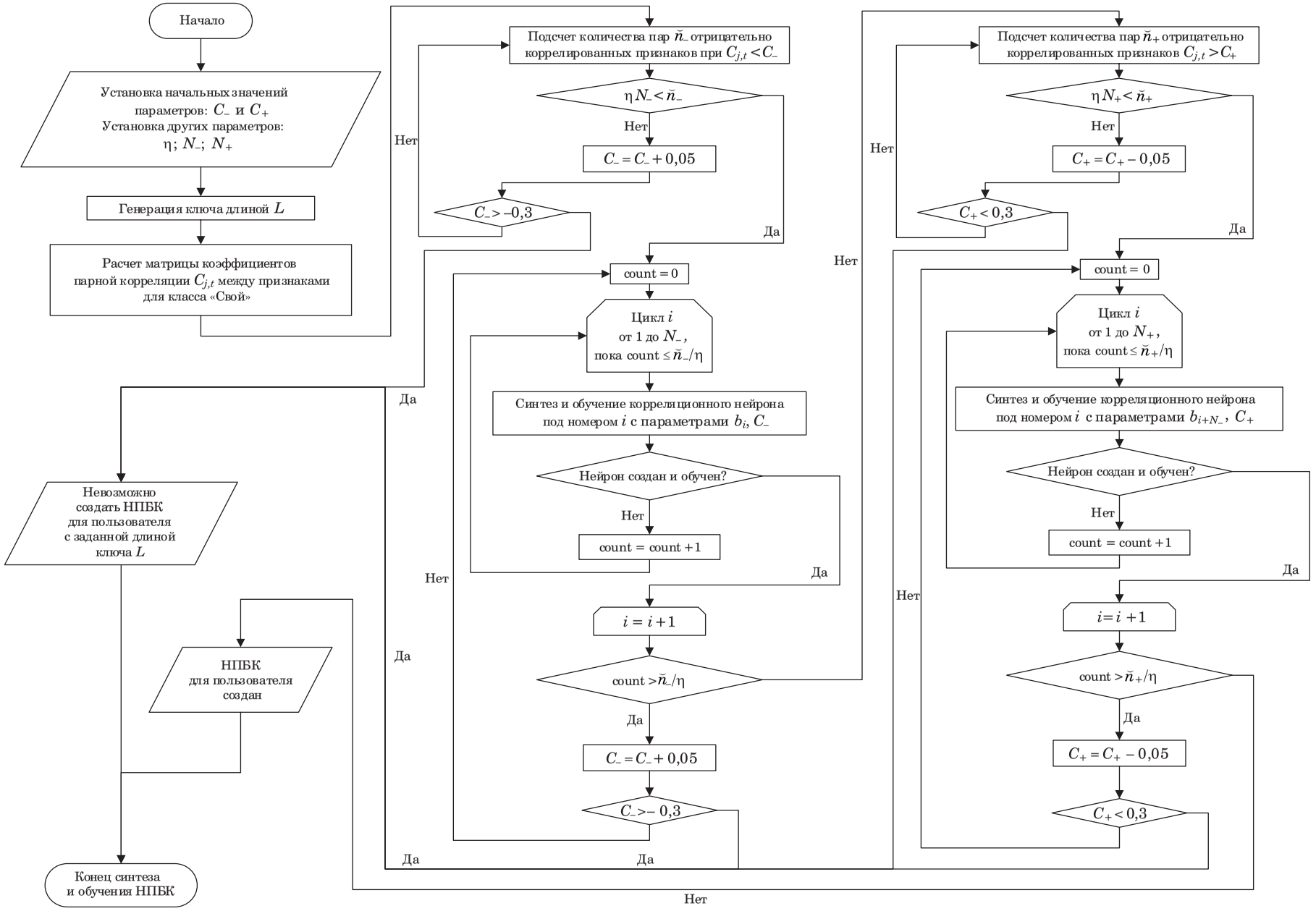
$$F(y) = \int_{-\infty}^{y} \frac{1}{\varsigma\sqrt{2\pi}} e^{-\frac{(\zeta-\xi)^2}{2\varsigma^2}} \mathrm{d}\zeta, \qquad (9)$$

где ξ и ς — математическое ожидание и среднеквадратичное отклонение величины y при поступлении на входы нейрона обучающих примеров «Свой» или «Чужие».

Исходя из гипотезы о нормальном распределении y, подтвержденной методом хи-квадрат [1], каждый нейрон будет давать ложный отказ пользователям «Свой» с вероятностью, в среднем не превышающей 0,002. Однако в силу наличия корреляции между откликами различных нейронов показатели FRR и FAR невозможно просчитать заранее без проведения численного эксперимента.



■ ***Рис. 7.*** Алгоритм синтеза и обучения корреляционного нейрона
■ ***Fig. 7.*** Algorithm for synthesis and training of a correlation neuron



■ ***Рис. 8.*** Алгоритм синтеза и обучения НПБК

■ ***Fig. 8.*** Algorithm for synthesis and training of biometrics-code converter

Настройка порогов нейрона выполняется по модифицированному алгоритму (рис. 7, базовый алгоритм представлен в работе [1]).

Выходы кодировщика должны быть преобразованы в мета-признаки (4), которые должны быть связаны с НПБК. При регистрации нового пользователя для него создается отдельный НПБК, который обучается на примерах «Свой» и «Чужие» в доверенной среде в соответствии с алгоритмом, представленным на рис. 8. После обучения НПБК может размещаться в открытом виде.

Таблицы порогов T весовых коэффициентов w_i обученного НПБК представляют собой защищенный эталон пользователя.

Эксперименты по распознаванию голосовых образов

При проведении эксперимента использованы предложенные модели предварительно обученных нами автокодировщиков, модель НПБК на базе корреляционных нейронов, предложенный алгоритм ее обучения (см. рис. 8) и сформированный в рамках настоящей работы набор данных.

При оценке на собственной базе для обучения каждого НПБК использовано по 20 примеров «Свой» голосового образа определенного пользователя, находящегося в нормальном состоянии, а также по одному примеру всех остальных пользователей из группы «Зарегистрированные субъекты» в качестве тренировочной выборки «Чужие» (всего 64 примера «Чужих»). При оценке на базе RedDots для обучения использовано по 10 примеров «Свой» и 239 примеров «Чужих».

Для тестирования НПБК и определения вероятности ошибок «ложного отказа» «Своему» (FRR) использованы образы «Свой», не участвовавшие в обучении. Эта серия опытов выполнялась дважды: сначала с использованием образов, полученных на первом этапе сбора данных, когда состояние пользователей было нормальным (без дрейфа), потом с использованием образов, полученных позже в измененных состояниях субъектов (в условиях дрейфа).

Для тестирования стойкости НПБК к попыткам входа со стороны злоумышленника и определения вероятности ошибок «ложного допуска» (FAR) использованы примеры из группы «Неизвестные Чужие» для оценки на собственной базе (и «Imposters» для оценки на RedDots). Результаты тестирования можно видеть в табл. 1 и 2.

Балансировка показателей FRR и FAR возможна за счет использования кодов, исправляющих ошибки, например кодов Безяева [24]. С их помощью можно исправить определенное количество ошибок в формируемом на выходе НПБК ключе и таким образом установить порог принятия биометрического образа.

Нейросетевой преобразователь биометрия-код на базе корреляционных нейронов дает гораздо меньший процент ошибок и в разы большую длину ключа, чем классический НПБК на базе алгоритма обучения ГОСТ Р 52633.5. Влияние состояния субъекта на результаты аутентификации при использовании предложенной модели НПБК менее существенны, чем для классической модели. Полученные результаты можно объяснить тем, что если дрейфующие характеристики голоса коррелированы, то они изменяются схожим образом. Другими словами, корреляция между существенной частью дрейфующих признаков сохраняется. По этой причине корреляционные нейроны являются относительно устойчивыми к дрейфу голосовых образов.

Из представленных результатов видно, что предложенная модель дает уровни ошибок и точ-

■ ***Таблица 1.*** Результаты эксперимента с собственной базой дикторов (EER, %)
■ ***Table 1.*** Experimental results with its own base of speakers (EER, %)

η	Предложенная модель НПБК при количестве нейронов N				НПБК, обучаемый по ГОСТ Р 52633.5, при количестве нейронов N			
	512		1024		128		256	
	1	2	1	2	1	2	1	2
2	–	–	–	–	7,73	8,91	5,27	7,9
4	4,31	5,38	3,7	4,69	7,46	10,73	–	–
6	3,64	4,73	3,47	4,41	–	–	–	–
7	3,42	4,46	3,33	4,31	–	–	–	–
8	3,66	4,72	3,26	4,33	–	–	–	–
9	3,75	4,76	3,48	4,42	–	–	–	–

Примечание: Столбцы 1 — дрейфа нет; столбцы 2 — дрейф есть.

■ ***Таблица 2.*** Результаты эксперимента с набором данных RedDots
■ ***Table 2.*** Experimental results with RedDots dataset

Методы и модели	EER, %	Точность,%
Комплексирование нескольких моделей и методов (модель гауссовой смеси, i-, x-vector) [25]	2,77	–
Вейвлет-преобразование, нейронная сеть и преобразование Гильберта [26]	–	95,1
MFCC + глубокая нейронная сеть [27]	1,61	–
Глубокие скрытые марковские модели (DHMM) [28]	–	97,6
Иерархическая многослойная акустическая модель (HiLAM) [29]	1,02	–
Предложенная модель НПБК (η =6, N = 4096)	2,64	97,36

ности, сопоставимые с мировым уровнем. Однако стоит учитывать, что в настоящем исследовании дополнительно ставится задача не только защиты от дрейфа, но и защиты биометрических шаблонов от компрометации, а также обеспечения автоматического и робастного обучения при регистрации нового пользователя. Все указанные свойства одновременно не обеспечиваются ни одной из указанных моделей, с которыми осуществлялось сравнение по базе RedDots.

Заключение

Полученные результаты показали, что есть преимущества от использования корреляционных нейронов в задачах голосовой биометрии:

– данные о классе «Свой» не компрометируются, так как их не требуется хранить в виде параметров распределения значений признаков;

– НПБК на базе корреляционных нейронов дает меньший процент ошибок (почти на 60 %) и большую длину ключа (в четыре раза) по сравнению с НПБК на базе ГОСТ Р 52633.5. Количество ошибок составило: EER = 3,26 % (для предложенной модели) при длине ключа 1024 бит и EER = 5,27 % (для классической модели) при длине ключа 256 бит;

– если дрейфующие признаки сильно коррелированы, то обычно они сдвигаются синхронно по диагонали (чаще всего в рамках линии расширения пространства признаков, см. рис 5, *б*), при этом значение мета-признака меняется несущественно. Эксперимент показал, что это справедливо, так как вероятности ошибок повышаются в среднем на 25–30 % (для классической модели повышение количества ошибок при изменении состояния пользователя колеблется от 15 до 50 %);

– предложенная модель не уступает существующим аналогам по точности, при этом существующие модели не обеспечивают защиту биометрических шаблонов и автоматическое обучение при регистрации нового пользователя, о чем свидетельствуют эксперименты на открытой базе RedDots.

Дальнейшие исследования будут направлены на создание гибридных моделей нейронных сетей, способных выполняться в защищенном режиме, и НПБК на их основе. Если объединить классические нейроны с другими типами нейронов в гибридный слой нейронов, синтезировав гибридную нейронную сеть, можно снизить показатели FRR и FAR и повысить энтропию ответов НПБК. Еще более интересным является то, что создание многослойных гибридных нейронных сетей, где в каждом слое будут использованы различные типы нейронов, может также позволить снизить вероятность ошибочных решений и открыть новые перспективы.

Финансовая поддержка

Работа выполнена ОмГТУ в рамках государственного задания Минобрнауки России на 2023–2025 годы № FSGF-2023-0004.

Литература

1. **Sulavko A. E.** Biometric-based key generation and user authentication using acoustic characteristics of the outer ear and a network of correlation neurons. *Sensors*, 2022, vol. 22, pp. 9551. doi:10.3390/s22239551
2. **Иванов А. И., Князьков В. С.** Перспектива многократного увеличения ресурсов доверенных вычислений за счет привлечения гибрида нейросетевой обработки биометрии и гомоморфного шифрования. *Состояние и перспективы развития современной науки по направлению «Техническое зрение, распознавание образов»: материалы III Всерос. науч.-техн. конф.*, Анапа, 18 марта 2021 г. Анапа, 2021, с. 173–176. EDN: WFBSXO
3. **Catak F. O., Yayilgan S. Y., Abomhara M.** A privacy-preserving fully homomorphic encryption and parallel computation based biometric data matching. *Preprints*

2020, No. 2020070658. doi:10.20944/preprints202007.0658.v1

4. **Barrero G. M., Maiorana E., Galbally J., Campisi P., Fierrez J.** Multi-biometric template protection based on Homomorphic Encryption. *Pattern Recognition*, 2017, vol. 67, pp. 149–163.
5. **Torres W. A. A., Bhattacharjee N., Srinivasan B.** Effectiveness of fully homomorphic encryption to preserve the privacy of biometric data. *Proc. of the 16th Intern. Conf. on Information Integration and Web-based Applications & Services (iiWAS '14)*, N. Y., USA, 2014, pp. 152–158. doi:https://doi.org/10.1145/2684200.2684296
6. **Sudhakar T., Gavrilova M.** Cancelable biometrics using deep learning as a cloud service. *IEEE Access*, 2020, vol. 8, pp. 112932–112943. doi:10.1109/ACCESS.2020.3003869
7. **El-Shafai W., Mohamed F. A. H. E., Elkamchouchi H. M., Abd-Elnaby M., Elshafee A.** Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm. *IEEE Access*, 2021, vol. 9, pp. 77675–77692.
8. **Ponce-Hernandez W., Blanco-Gonzalo R., Liu-Jimenez J., Sanchez-Reillo R.** Fuzzy vault scheme based on fixed-length templates applied to dynamic signature verification. *IEEE Access*, 2020, vol. 8, pp. 11152–11164.
9. **Rathgeb C., Merkle J., Scholz J., Tams B., Nesterowicz V.** Deep face fuzzy vault: Implementation and performance. *Computers & Security*, 2022, vol. 113, Article 102539.
10. **Иванов А. И.** *Нейросетевая защита конфиденциальных биометрических образов гражданина и его личных криптографических ключей*: монография. Пенза, ПНИЭИ, 2014. 57 с.
11. **Ахметов Б. С., Иванов А. И., Фунтиков В. А., Безяев А. В., Малыгина Е. А.** *Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа*: монография. Алматы, Издательство LEM, 2014. 144 с.
12. **Marshalko G. B.** On the security of a neural network-based biometric authentication scheme. *Математические вопросы криптографии*, 2014, т. 5, № 2, с. 87–98. EDN: TKJPFV
13. **Иванов А. И., Крохин И. А.** Таблица вероятности появления разных стартовых условий для атак Маршалко на нейроны с общими входными связями. *Состояние и перспективы развития современной науки по направлению «Техническое зрение, распознавание образов»: материалы III Всерос. науч.-техн. конф.*, Анапа, 18 марта 2021 г. Анапа, 2021, с. 171–172.
14. **Сулавко А. Е.** Высоконадежная двухфакторная биометрическая аутентификация по рукописным и голосовым паролям на основе гибких нейронных сетей. *Компьютерная оптика*, 2020, т. 44, № 1, с. 82–91. doi:10.18287/2412-6179-CO-567, EDN: OVLPUD
15. **Bogdanov D. S., Mironkin V. O.** Data recovery for a neural network-based biometric authentication scheme. *Математические вопросы криптографии*, 2019, т. 10, № 2, с. 61–74.
16. **Сулавко А. Е., Еременко А. В., Борисов Р. В., Иниватов Д. П.** Влияние психофизиологического состояния диктора на параметры его голоса и результаты биометрической аутентификации по речевому паролю. *Компьютерные инструменты в образовании*, 2017, № 4, с. 29–47.
17. **Sheluhin O. I., Erokhin S. D., Osin A. V., Barkov V. V.** Experimental studies of network traffic of mobile devices with Android OS. *IEEE Conf. "Systems of Signals Generating and Processing in the Field of on Board Communications"*, Moscow, Russia, 20–21 March 2019. IEEE, 2019, pp. 1–4. doi:10.1109/SOSG.2019.8706824
18. **Sheluhin O. I., Barkov V. V., Sekretarev S. A.** The online classification of the mobile applications traffic using data mining techniques. *T-Comm*, 2019, vol. 13, no. 10, pp. 60–67. doi:10.24411/2072-8735-2018-10317.1
19. **Николенко С. И., Кадурин А. А., Архангельская Е. О.** *Глубокое обучение. Погружение в мир нейронных сетей*. СПб., Питер, 2018. 480 с.
20. **Lee K. A., Larcher A., Wang G., Kenny P., Brümmer N., van Leeuwen D., Aronowitz H., Kockmann M., Vaquero C., Ma B., Li H., Stafylakis T., Alam M. J., Swart A., Perez J.** The reddots data collection for speaker recognition. *Proc. Interspeech 2015*, 2015, pp. 2996–3000. doi:10.21437/Interspeech.2015-95
21. **Snyder D., Garcia-Romero D., Sell G., Povey D., Khudanpur S.** X-vectors: Robust DNN embeddings for speaker recognition. *IEEE Intern. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, Calgary, AB, Canada, 15–20 April 2018. IEEE, 2018, pp. 5329–5333. doi:10.1109/ICASSP.2018.8461375
22. **Nagrani A., Chung J. S., Xie W., Zisserman A.** Voxceleb: Large-scale speaker verification in the wild. *Computer Speech & Language*, 2020, vol. 60, Article 101027.
23. **Дагаева М. В., Катасева Д. В., Катасев А. С.** Аугментация данных и построение нейросетевых моделей распознавания рукописных символов в системах биометрической аутентификации. *Информация и безопасность*, 2018, т. 21, № 3, с. 366–371.
24. **Безяев А. В.** Биометрико-нейросетевая аутентификация: обнаружение и исправление ошибок в длинных кодах без накладных расходов на избыточность: препринт. Пенза, Изд-во ПГУ, 2020. 40 с.
25. **Sarkar A. K., Tan Z. H.** *On bottleneck features for text-dependent speaker verification using X-vectors*. arXiv preprint arXiv:2005.07383. 2020.
26. **Sarma K., Pyrtuh F., Chakraborty D.** Speaker verification system using wavelet transform and neural network for short utterances. *Asian Journal*

for Convergence in Technology (AJCT), 2020, vol. 6, no. 1, pp. 30–35.
27. **Sarkar A. K., Tan Z. H.** Self-segmentation of pass-phrase utterances for deep feature learning in text-dependent speaker verification. *Computer Speech & Language*, 2021, vol. 70, Article 101229.
28. **Arora S. V., Vig R.** An efficient text-independent speaker verification for short utterance data from Mobile devices. *Multimedia Tools and Applications*, 2020, vol. 79, pp. 3049–3074.
29. **Laskar M. A., Laskar R. H.** HiLAM-state discriminative multi-task deep neural network in dynamic time warping framework for text-dependent speaker verification. *Speech Communication*, 2020, vol. 121, pp. 29–43.

UDC 004.93'1
doi:10.31799/1684-8853-2024-2-21-38
EDN: YIVAYM

Authentication based on voice passwords with the biometric template protection using correlation neurons

A. E. Sulavko[a], PhD, Tech., Associate Professor, orcid.org/0000-0002-9029-8028, sulavich@mail.ru
D. P. Inivatov[a], Assistant Professor, https://orcid.org/0000-0001-9911-1218
V. I. Vasilyev[b], Dr. Sc., Tech., Professor, orcid.org/0000-0002-6105-5481
P. S. Lozhnikov[a], Dr. Sc., Tech., Professor, orcid.org/0000-0001-7878-1976
[a]Omsk State Technical University, 11, Mira Pr., 644050, Omsk, Russian Federation
[b]Ufa University of Science and Technology, 32, Z. Validi St., 450076, Ufa, Russian Federation

Introduction: The issue of protecting biometric data from compromise is closely related to performance issues. Existing methods of biometric voice authentication either do not protect voice data from compromise or give a high percentage of erroneous decisions; in addition, they do not provide resistance to voice image drift. **Purpose:** To develop a method of biometric voice authentication that is resistant to the drift of biometric data while ensuring the confidentiality of voice parameters. **Results:** We propose an authentication method using neural network "biometrics-to-code" converters based on a modified model of correlation neurons and their training algorithms. It has been established that correlations between features contain information about images that does not duplicate the information contained in the features. The biometrics-to-code converter based on correlation neurons produces a much lower percentage of errors and several times longer key length than the classical model based on the GOST R 52633.5 learning algorithm. The number of errors was: 3.26%. When the subject's state changes (intoxication or sleepiness), the number of errors for the developed method does not increase as significantly as for the classical model of the biometrics-code neural network converter. **Practical relevance:** The results can be used to increase the security of computer resources from unauthorized access and biometric data from compromise. **Discussion:** Combining neurons of various types into a single layer will make it possible to create more stable and reliable biometric-to-code neural network converters.

Keywords — secure execution of neural network algorithms, processing of correlated biometric features, voice biometrics, neural network biometrics-to-code converters, time series analysis, autoencoders.

For citation: Sulavko A. E., Inivatov D. P., Vasilyev V. I., Lozhnikov P. S. Authentication based on voice passwords with the biometric template protection using correlation neurons. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 21–38 (In Russian). doi:10.31799/1684-8853-2024-2-21-38, EDN: YIVAYM

Financial support
The research was supported by Ministry of Science and Higher Education of the Russian Federation (theme No. FSGF-2023-0004).

References

1. Sulavko A. E. Biometric-based key generation and user authentication using acoustic characteristics of the outer ear and a network of correlation neurons. *Sensors*, 2022, vol. 22, pp. 9551. doi:10.3390/s22239551
2. Ivanov A. I., Knyazkov V. S. The prospect of a multiple increase in trusted computing resources by involving a hybrid of neural network processing of biometrics and homomorphic encryption. *Materialy III Vseros. nauch.-tekhn. konf. «Sostoyanie i perspektivy razvitiya sovremennoj nauki po napravleniyu "Tekhnicheskoe zrenie, raspoznavanie obrazov"»* [Proc. III All-Russian Scient.-Tech. Conf. «The State and prospects of development of modern science in the direction of "Technical vision, pattern recognition"»], Anapa, 2021, pp. 173–176 (In Russian). EDN: WFBSXO
3. Catak F. O., Yayilgan S. Y., Abomhara M. A privacy-preserving fully homomorphic encryption and parallel computation based biometric data matching. *Preprints* 2020, No. 2020070658. doi:10.20944/preprints202007.0658.v1
4. Barrero G. M., Maiorana E., Galbally J., Campisi P., Fierrez J. Multi-biometric template protection based on Homomorphic Encryption. *Pattern Recognition*, 2017, vol. 67, pp. 149–163.
5. Torres W. A. A., Bhattacharjee N., Srinivasan B. Effectiveness of fully homomorphic encryption to preserve the privacy of biometric data. *Proc. of the 16th Intern. Conf. on Information Integration and Web-based Applications & Services (iiWAS '14)*, N. Y., USA, 2014, pp. 152–158. doi:https://doi.org/10.1145/2684200.2684296
6. Sudhakar T., Gavrilova M. Cancelable biometrics using deep learning as a cloud service. *IEEE Access*, 2020, vol. 8, pp. 112932–112943. doi:10.1109/ACCESS.2020.3003869
7. El-Shafai W., Mohamed F. A. H. E., Elkamchouchi H. M., Abd-Elnaby M., Elshafee A. Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm. *IEEE Access*, 2021, vol. 9, pp. 77675–77692.
8. Ponce-Hernandez W., Blanco-Gonzalo R., Liu-Jimenez J., Sanchez-Reillo R. Fuzzy vault scheme based on fixed-length templates applied to dynamic signature verification. *IEEE Access*, 2020, vol. 8, pp. 11152–11164.
9. Rathgeb C., Merkle J., Scholz J., Tams B., Nesterowicz V. Deep face fuzzy vault: Implementation and performance. *Computers & Security*, 2022, vol. 113, pp. 102539.

10. Ivanov A. I. *Neirosetevaia zashchita konfidentsial'nykh biometricheskikh obrazov grazhdanina i ego lichnykh kriptograficheskikh kliuchei* [Neural Protection of Sensitive Biometric Images of the Citizen and his Personal Cryptographic Keys]. Penza, PNIEI Publ., 2014. 57 p. (In Russian).
11. Ahmetov B. S., Ivanov A. I., Funtikov V. A., Bezjaev A. V., Malygina E. A. *Tekhnologiia ispol'zovaniia bol'shikh neironnykh setei dlia preobrazovaniia nechetkikh biometricheskikh dannykh v kod kliucha dostupa* [Technology of Using Large Neural Networks for Fuzzy Transformation of Biometric Data in the Access Code Key]. Almaty, LEM Publ., 2014. 144 p. (In Russian).
12. Marshalko G. B. On the security of a neural network-based biometric authentication scheme. *Mathematical Aspects of Cryptography*, 2014, vol. 5, no. 2, pp. 87–98. EDN: TKJPFV
13. Ivanov A. I., Krokhin I. A. Table of the probability of occurrence of different starting conditions for Marshalko attacks on neurons with common input connections. *Materialy III Vseros. nauch.-tekhn. konf. «Sostoyanie i perspektivy razvitiya sovremennoj nauki po napravleniyu "Tekhnicheskoe zrenie, raspoznavanie obrazov"»* [Proc. III All-Russian Scient.-Tech. Conf. «The State and prospects of development of modern science in the direction of "Technical vision, pattern recognition"»], Anapa, 2021, pp. 171–172 (In Russian).
14. Sulavko A. E. Highly reliable two-factor biometric authentication by handwritten and voice passwords based on flexible neural networks. *Computer optics*, 2020, vol. 44, no. 1, pp. 82–91 (In Russian). doi:10.18287/2412-6179-CO-567, EDN: OVLPUD
15. Bogdanov D. S., Mironkin V. O. Data recovery for a neural network-based biometric authentication scheme. *Mathematical Aspects of Cryptography*, 2019, vol. 10, no. 2, pp. 61–74.
16. Sulavko A. E., Eremenko A. V., Borisov R. V., Inivatov D. P. Influence of a speaker's psycho-physiological state to his voice parameters and results of biometric authentication by speech enabled password. *Computer Tools in Education*, 2017, no. 4, pp. 29–47 (In Russian).
17. Sheluhin O. I., Erokhin S. D., Osin A. V., Barkov V. V. Experimental studies of network traffic of mobile devices with Android OS. *IEEE Conf. "Systems of Signals Generating and Processing in the Field of on Board Communications"*, Moscow, Russia, 20–21 March 2019. IEEE, 2019, pp. 1–4. doi:10.1109/SOSG.2019.8706824
18. Sheluhin O. I., Barkov V. V., Sekretarev S. A. The online classification of the mobile applications traffic using data mining techniques. *T-Comm*, 2019, vol. 13, no. 10, pp. 60–67. doi:10.24411/2072-8735-2018-10317.1
19. Nikolenko S. I., Kadurin A. A., Arkhangelskaya E. O. *Glubokoe obuchenie. Pogruzhenie v mir nejronnyh setej* [Deep learning. Dive into the world of neural networks]. Saint-Petersburg, Piter Publ., 2018. 480 p. (In Russian).
20. Lee K. A., Larcher A., Wang G., Kenny P., Brümmer N., van Leeuwen D., Aronowitz H., Kockmann M., Vaquero C., Ma B., Li H., Stafylakis T., Alam M. J., Swart A., Perez J. The reddots data collection for speaker recognition. *Proc. Interspeech 2015*, 2015, pp. 2996–3000. doi:10.21437/Interspeech.2015-95
21. Snyder D., Garcia-Romero D., Sell G., Povey D., Khudanpur S. X-vectors: Robust DNN embeddings for speaker recognition. *IEEE Intern. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, Calgary, AB, Canada, 15–20 April 2018. IEEE, 2018, pp. 5329–5333. doi:10.1109/ICASSP.2018.8461375
22. Nagrani A., Chung J. S., Xie W., Zisserman A. Voxceleb: Large-scale speaker verification in the wild. *Computer Speech & Language*, 2020, vol. 60, Article 101027.
23. Dagaeva M. V., Kataseva D. V., Katasev A. S. Data augmentation and construction of neural network models for handwritten character recognition in biometric authentication systems. *Informaciya i bezopasnost'*, 2018, vol. 21, no. 3, pp. 366–371 (In Russian).
24. Bezyaev A. V. *Biometriko-neyrosetevaya autentifikatsiya: obnaruzhenie i ispravlenie oshibok v dlinnykh kodakh bez nakladnykh raskhodov na izbytochnost'* [Bio-metrical neural network authentication: detecting and correcting errors in long codes without the overhead of redundancy]. Penza, PGU Publ., 2020. 40 p. (In Russian).
25. Sarkar A. K., Tan Z. H. *On bottleneck features for text-dependent speaker verification using X-vectors*. arXiv preprint arXiv:2005.07383. 2020.
26. Sarma K., Pyrtuh F., Chakraborty D. Speaker verification system using wavelet transform and neural network for short utterances. *Asian Journal for Convergence in Technology (AJCT)*, 2020, vol. 6, no. 1, pp. 30–35.
27. Sarkar A. K., Tan Z. H. Self-segmentation of pass-phrase utterances for deep feature learning in text-dependent speaker verification. *Computer Speech & Language*, 2021, vol. 70, Article 101229.
28. Arora S. V., Vig R. An efficient text-independent speaker verification for short utterance data from Mobile devices. *Multimedia Tools and Applications*, 2020, vol. 79, pp. 3049–3074.
29. Laskar M. A., Laskar R. H. HiLAM-state discriminative multi-task deep neural network in dynamic time warping framework for text-dependent speaker verification. *Speech Communication*, 2020, vol. 121, pp. 29–43.