http://vestnik.mrsu.ru
ISSN Print 0236-2910
ISSN Online 2313-0636
УДК 531.1:519.854
DOI: 10.15507/0236-2910.027.201702.224-238

КВАНТОВАЯ СУПЕРПОЗИЦИЯ ДИСКРЕТНОГО СПЕКТРА СОСТОЯНИЙ МАТЕМАТИЧЕСКОЙ МОЛЕКУЛЫ КОРРЕЛЯЦИИ ДЛЯ МАЛЫХ ВЫБОРОК БИОМЕТРИЧЕСКИХ ДАННЫХ

В. И. Волчихин[1], А. И. Иванов[2*], А. В. Сериков[3], Ю. И. Серикова[1]
[1]ФГБОУ ВО «Пензенский государственный университет» (г. Пенза, Россия)
[2]АО «Пензенский научно-исследовательский электротехнический институт» (г. Пенза, Россия)
[3]АО «Рубин» (г. Пенза, Россия)
[*]bio.ivan.penza@mail.ru

Введение. Целью работы является снижение количества ошибок при вычислении коэффициентов корреляции на малых тестовых выборках.
Материалы и методы. Для получения функций плотности распределения значений коэффициентов корреляции на малых выборках были использованы средства имитационного моделирования. Предложен метод квантования данных, позволяющий получить дискретный спектр состояний одного из разновидностей корреляционных функционалов. Данная операция позволяет рассматривать предложенную конструкцию как математическую корреляционную молекулу, описывающуюся некоторым аналогом континуально-квантового уравнения Шредингера.
Результаты исследования. Ранее было показано, что хи-квадрат молекула Пирсона на малых выборках позволяет усилить мощность классического хи-квадрат критерия до 20 раз. Описанная в данной статье математическая корреляционная молекула обладает аналогичными свойствами и в будущем позволит снизить ошибки вычисления классических коэффициентов корреляции на малых выборках.
Обсуждение и заключения. Сделано предположение, что существует бесконечное множество математических молекул, похожих по их свойствам на реальные физические молекулы. Уравнение Шредингера не уникально, и для каждой математической молекулы может быть построен его аналог. Можно ожидать синтеза математических молекул для большого количества уже известных статистических критериев и статистических моментов. Все вышеперечисленное предположительно позволить снизить количество ошибок расчетов, обусловленных квантовыми эффектами, возникающими на малых тестовых выборках.

Ключевые слова: коэффициент корреляции, квантовая суперпозиция, молекула, дискретный спектр состояний, статистический анализ, малая выборка

Для цитирования: Квантовая суперпозиция дискретного спектра состояний математической молекулы корреляции для малых выборок биометрических данных / В. И. Волчихин [и др.] // Вестник Мордовского университета. 2017. Т. 27, № 2. С. 224–238. DOI: 10.15507/0236-2910.027.201702.224-238

© Волчихин В. И., Иванов А. И., Сериков А. В., Серикова Ю. И., 2017

QUANTUM SUPERPOSITION OF THE DISCRETE SPECTRUM OF MATHEMATICAL CORRELATION MOLECULE STATUS FOR SMALL SAMPLES OF BIOMETRIC DATA

V. I. Volchikhin[a], A. I. Ivanov[b*], A. V. Serikov[c], Yu. I. Serikova[a]

[a]Penza State University (Penza, Russia)
[b]Penza Electrotechnical Research Institute (Penza, Russia)
[c]Joint-Stock Company Rubin (Penza, Russia)
[*]bio.ivan.penza@mail.ru

Introduction. The study promotes to decrease a number of errors of calculating the correlation coefficient in small test samples.
Materials and Methods. We used simulation tool for the distribution functions of the density values of the correlation coefficient in small samples. A method for quantization of the data, allows obtaining a discrete spectrum states of one of the varieties of correlation functional. This allows us to consider the proposed structure as a mathematical correlation molecule, described by some analogue continuous-quantum Schrödinger equation.
Results. The chi-squared Pearson's molecule on small samples allows enhancing power of classical chi-squared test to 20 times. A mathematical correlation molecule described in the article has similar properties. It allows in the future reducing calculation errors of the classical correlation coefficients in small samples.
Discussion and Conclusions. The authors suggest that there are infinitely many mathematical molecules are similar in their properties to the actual physical molecules. Schrödinger equations are not unique, their analogues can be constructed for each mathematical molecule. You can expect a mathematical synthesis of molecules for a large number of known statistical tests and statistical moments. All this should make it possible to reduce calculation errors due to quantum effects that occur in small test samples.

Keywords: correlation coefficient, quantum superposition, molecule, discrete spectrum states, statistical analysis of small samples

For citation: Volchikhin V. I., Ivanov A. I., Serikov A. V., Serikova Yu. I. Quantum superposition of the state discrete spectrum of mathematical correlation molecule for small samples of biometric data. *Vestnik Mordovskogo universiteta* = Mordovia University Bulletin. 2017; 2(27):224-238. DOI: 10.15507/0236-2910.027.201702.224-238

Введение

При проведении экспериментальных исследований далеко не всегда удается получить достаточный объем информации. Например, изучение биологических данных, сопутствующих редким заболеваниям, не может быть обосновано в рамках существующих статистических методик. В частности, применение стандартизованной методики проверки статистических гипотез по критерию хи-квадрат[1] строится на выборках, состоящих из ≥ 400 опытов. Существуют иные статистические критерии[2],

[1] ГОСТ Р 50.1.037-2001. Рекомендации по стандартизации. Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим : ч. I. Критерии типа $\chi 2$. М., 2001. 140 с. URL: http://www.complexdoc.ru/ntdpdf/541018/prikladnaya_statistika_pravila_proverki_soglasiya_opytnogo_raspredeleniya.pdf

[2] ГОСТ Р 50.1.037-2002. Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим : ч. II. Непараметрические критерии. М., 2002. 123 с. URL: https://znaytovar.ru/gost/2/R_5010372002_Prikladnaya_stati.html

менее требовательные к объему тестовой выборки, однако они имеют недостаточно высокую мощность на малых выборках.

Когда речь идет о биологах, изучающих редких животных, или ботаниках, изучающих редкие растения, научная общественность смирилась (де-факто) с отсутствием достаточных объемов статистики по объективным причинам. Для медиков проблема сбора достаточных статистических данных по редким заболеваниям стоит значительно более остро, особенно когда речь идет о редких инфекционных заболеваниях и тестировании новых лекарств.

Еще одной наукой, сталкивающейся с проблемами малых выборок, является биометрия. В период с 1901 г. до конца XX в. статистический журнал «Biometrika» (Оксфорд) играл ведущую роль в освещении материала по проблемам малых выборок. В XXI в. биометрия продолжает занимать лидирующее положение по обучению и тестированию преобразователей «Биометрия – код доступа» на малых выборках. При этом объем затрачиваемых средств на биометрию и значимость решаемых биометрией задач ежегодно увеличивается. В США биометрические технологии регулируются ~ 100 национальными стандартами и приблизительно таким же числом международных стандартов. В Российской Федерации было введено 7 национальных биометрических стандартов и адаптировано около 50 международных.

В данной статье отражены последние тенденции развития обработки многомерных биометрических данных, связанные со стремлением решить проблему малых выборок за счет перехода к программной поддержке квантовой суперпозиции при вычислении коэффициентов корреляции.

Обзор литературы

Проблемам малых выборок (обучающих и/или тестовых) в биометрии уделяется значительное внимание в связи с тем, что эти показатели напрямую связаны с эффективностью работы биометрической системы. В США, Канаде, Евросоюзе защита и преобразование биометрических данных осуществляется т. н. «нечеткими экстракторами» [1–3], которые по своим параметрам значительно уступают искусственным нейронным сетям [4]. Применение нейросетевых преобразователей биометрии в код доступа, а также тестирование качества работы нейросетевых преобразователей регламентируются стандартами[3-4].

Последний стандарт уникален тем, что он построен на использовании эффектов квантовой суперпозиции при анализе выходных данных искусственной нейронной сети. Именно по этой причине для оценки вероятности ошибок второго рода на уровне 0.000 000 1 стандарт рекомендует использовать всего 32 примера разных биометрических образов «Чужой». Из-за применения новых вычислительных технологий вместо проведения 1 000 000 тестовых опытов достаточно применить всего 32. Мы наблюдаем огромное сокращение объема тестовой выборки и, соответственно, трудозатрат на тестирование из-за отказа от простого статистического перебора в пользу перехода к использованию квантового оракула, предсказывающего вероятности событий по малой выборке.

Следует подчеркнуть, что первоначально квантовая математика разрабатывалась с другой целью. В 1980 г.

[3] ГОСТ Р 52633-2006. URL: http://www.internet-law.ru/gosts/gost/456

[4] ГОСТ Р 52633.3-2011. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора. URL: http://vsegost.com/Catalog/52/2633.shtml

Ю. И. Манин[5] первым осознал возможности квантовых вычислительных машин, занимаясь теорией струн. Приблизительно на 50 лет раньше физики столкнулись с тем, что планетарная модель атома «не работает». Бору пришлось вводить гипотезу поглощения и излучения энергии квантами. Позднее задача была формализована в виде уравнения Шредингера, имеющего квантово-волновые решения. Развитие физики и математики привело к тому, что оба направления исследований практически объединились в рамках теории струн[6]. Фотоны, кварки, фермионы, бозоны, струны на микроуровне (при Платковских длинах) и суперструны на галактическом макроуровне являются квантовым свойством континуума пространства-времени. Многомерные физически существующие пространственно-временные континуумы всегда каким-то образом самоквантуются (сами себя квантуют). Подобные эффекты несомненно могут быть использованы при создании квантовых вычислителей [5] в парадигме Манина-Шредингера или квантово-механических вычислителей.

Ожидаемые огромные скорости вычисления перспективных квантовых компьютеров породили создание ряда важнейших вычислительных алгоритмов, объединение которых позволяет говорить о появлении нового раздела математики – квантовой математики. Важнейшим свойством новой математики является возможность описания связи квантовой энтропии, квантовой суперпозиции и квантовой сцепленности[7–8] [6–7] в рамках квантовой информатики.

Непротиворечивое объединение нескольких базовых математических конструкций открыло новые возможности. Когда создавалась квантовая математика, не было другого пути, кроме использования волновых решений уравнения Шредингера и проверки на них новых математических соотношений. После того как элементы квантовой математики были созданы и проверены, использование хорошо изученного уравнения Шредингера стало не обязательным. Объекты, точно соответствующие уравнению Шредингера, очень трудно смоделировать на обычной вычислительной машине[8], однако существует множество других уравнений, похожих по создаваемым эффектам.

Одним из аналогов уравнения Шредингера является классический хи-квадрат критерий. Это становится очевидным, если применять его для малых выборок, противореча рекомендациям по стандартизации. Плотность распределения получаемых значений хи-квадрат критерия по мере снижения размеров тестовой выборки становится периодической. Однако если дополнительно выполнить условия синхронизации данных (привязать выбор положения столбцов гистограммы к математическому ожиданию выборки), то положение линий спектра состояний становился таким же стабильным, как положение спектральных линий у молекулы водорода. Таким образом, допустимо рассматривать хи-квадрат критерий как некоторую математическую молекулу [8–11], порождающую стабильный спектр

[5] **Манин Ю. И.** Вычислимое и невычислимое. Кибернетика. М. : Сов. радио, 1980. 128 с. URL: http://publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/_Manin_Yu.I..html#h

[6] **Кобзарев И. Ю., Манин Ю. И.** Элементарные частицы: диалоги физика и математика. М. : Фазис. 1997.

[7] **Холево А. С.** Введение в квантовую теорию информации. М. : МЦНМО. 2002. 128 с. URL: http://imash.ru/netcat_files/file/BIBLIO/Vtechnika/Холево%20A_C_%20-%20Введение%20в%20квантовую%20теорию%20информации%20-%202002.pdf

[8] **Нильсен М., Чанг И.** Квантовые вычисления и квантовая информация : монография. М. : Мир, 2006. 821 с.

выходных дискретных состояний при квантовании гистограммой некоторого внутреннего континуума непрерывных состояний.

Принципиальное преимущество в данном случае заключается в том, что состояния хи-квадрат молекулы, в отличие от уравнения Шредингера, моделируется всего несколькими строками программного кода. Это означает, что возможно организовать программный квантовый вычислитель, поддерживающий квантовую суперпозицию и квантовую запутанность, соответствующие хи-квадрат молекуле. За счет этого мы можем попытаться значительно усилить мощность хи-квадрат критерия на малых тестовых выборках. Уже созданный вариант такого программного усилителя позволяет за счет учета квантовых эффектов повысить мощность хи-квадрат критерия в 20 раз [11], то есть модифицированный хи-квадрат критерий на выборке из 20 опытов дает такие же вероятности ошибок, как стандартный хи-квадрат при 400 опытах. Предположительно усложнение программы из нескольких строк на языке программирования высокого уровня до нескольких тысяч строк позволит существенно повысить коэффициент усиления мощности критерия [10–11].

Следует отметить, что на молекуле хи-квадрат можно сгенерировать только специализированный вычислитель, усиливающий хи-квадрат критерий. Однако по аналогии с хи-квадрат молекулой возможно построение похожих на нее математических конструкций: эксцесс-молекулы, молекулы асимметрии, молекулы воды и т. д. В рамках данной статьи показывается возможность синтеза математической корреляционной молекулы. Все математические молекулы статистических моментов и критериев остаются узко специализированными вычислителями, поддерживающими эффекты квантовой суперпозиции только для одного статистического функционала на выборке фиксированного объема. Для каждого объема выборки статистические молекулы следует перестраивать (перепрограммировать), поскольку изменяется их спектр.

Для того чтобы сделать универсальный квантовый компьютер с целью решения произвольной задачи, необходимо уметь создавать квантовое обобщение частных квантовых вычислителей. Для этого применяются искусственные нейронные сети[9] и естественные нейронные сети [12].

Идея использования искусственных нейронных сетей для распознавания образов спектра разных математических молекул самоочевидна. Хи-квадрат молекула с внутренним континуумом нормальных состояний и хи-квадрат молекула с внутренним равновероятным континуумом состояний имеют разные спектры [10–11]. Достаточно научить одну нейронную сеть распознавать нормальный спектр, а другую нейронную сеть – распознавать спектр молекулы с равномерным внутренним континуумом. Эти две заранее обученные нейронные сети позволят классифицировать спектры любой другой наблюдаемой хи-квадрат молекулы. Каждая нейронная сеть будет решать только свою задачу, оценивая, насколько близок предъявленный спектр тому, чему ее заранее научили.

Отклики двух искусственных нейронных сетей позволяют найти расстояние предъявленного к распознаванию образа до первого базового образа (нормальный спектр) и до второго базового образа (равномерный спектр). Таким образом, вычисляется некото-

[9] **Иванов А. И.** Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции. Пенза : ПНИЭИ, 2016. 133 с. URL: http://пниэи.рф/activity/science/BOOK16.pdf.

рая нейросетевая метрика расстояний до двух уже известных спектров базовых образов, например, в пространстве расстояний Хэмминга[9].

Следует отметить, что задача обучения искусственных нейронных сетей в XX в. и в начале XXI в. рассматривалась как нетривиальная. Формально это положение сохранялось до принятия ГОСТ Р 52633.5-2011[10], завершившего 60-летний период эвристического создания множества алгоритмов обучения искусственных нейронных сетей. Алгоритмы, созданные по данной методике, оказались непригодны для быстрого, полностью автоматического обучения больших искусственных нейронных сетей, имеющих несколько сотен входов и 256[11] выходов. Абсолютное большинство созданных ранее алгоритмов обучения являются итерационными и потому не могут быть полностью автоматизированы. Кроме того, практически все старые алгоритмы обучения имеют экспоненциальную вычислительную сложность и, следовательно, непригодны для больших искусственных нейронных сетей.

Алгоритм обучения, принятый в ГОСТ Р 52633.5-2011, построен на создании случайных связей всех входов нейронной сети в целом и входов каждого из нейронов. Для каждого нейрона задается таблица связей путем обращения к программному генератору псевдослучайных целых чисел. Далее производится вычисление весового коэффициента каждого из входов k-го нейрона, исходя из знания математического ожидания входного биометрического параметра $E(\nu_i)$, его стандартного отклонения $s(\nu_i)$, а также знания о требуемом значении отклика нейрона «c_k»[12] на примере образа «Свой». Формально весовой коэффициент каждого из сети нейронов по данному стандартизованному алгоритму является функцией двух непрерывных переменных и одной дискретной переменной:

$$\mu_{j,k}(E(\nu_i),\sigma(\nu_i),"c_k") \text{ при } \begin{cases} 0 \le j \le 32, \\ 1 \le i \le 416\,;\,2048, \\ 0 \le k \le 255, \end{cases} \quad (1)$$

где j – номер входа сумматора нейрона; j – номер входа нейронной сети, не превышающие 416 для среды моделирования «БиоНейроАвтограф»[13] и 2 048 для рисунка радужной оболочки глаза [3]; переменные индексы j и i связаны между собой заранее заданной таблицей связей $T_k(i, j)$; k – номер нейрона в сети.

Такой алгоритм обучения является абсолютно устойчивым (легко автоматизируется), а его вычислитель-

[10] ГОСТ Р 52633.5-2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей «Биометрия – код доступа» URL: http://vsegost.com/Catalog/51/51407.shtml

[11] 256 бит – это длина ключа отечественных криптографических стандартов шифрования и формирования цифровой подписи, а также максимально допустимая длина пароля доступа в семействе ОС Windows

[12] С целью избегания путаницы дискретные переменные записывались в кавычках («c_k»), как это принято при программировании, а континуальные переменные – без них.

[13] **Иванов А. И., Захаров О. С.** Среда моделирования «БиоНейроАвтограф». URL: http://пниэи.рф/activity/science/noc.htm

ная сложность становится линейной, т. е. он может быть реализован даже на слабых процессорах мобильных устройств. Несмотря на то, что создание алгоритма обучения ГОСТ Р 52633.5-2011 является итогом почти 60-летних усилий большого количества исследователей, он далеко не идеален. Разработчики биометрических приложений стремятся, с одной стороны, уменьшить размеры обучающей выборки, а с другой стороны – повысить качество решений, принимаемых нейронной сетью. В связи с этим в РФ и Казахстане были инициированы исследования по созданию абсолютно устойчивых алгоритмов обучения больших искусственных нейронных сетей с квадратичной вычислительной сложностью[14] [13–19].

Формальная запись алгоритма для перспективного стандарта усложняется незначительно. Перспективный стандарт должен вычислять весовые коэффициенты каждого нейрона по более сложной формуле, дополнительно принимая во внимание коэффициенты корреляции контролируемых нейроном биометрических параметров:

$$\mu_{j,k}(E(\nu_i),\sigma(\nu_i),r(\nu_i,\nu_m),("c_k")), \quad (2)$$

где m – номер биометрического параметра, по отношению к которому вычисляется корреляция, данный номер должен определяться при обучении и храниться в таблице связей $T_k(i, j, m)$.

Проблема перехода от алгоритмов по ГОСТ Р 52633.5 (1) к перспективным алгоритмам обучения квадратичной сложности по формуле (2) сводится к повышению точности вычисления коэффициентов корреляции на малых выборках:

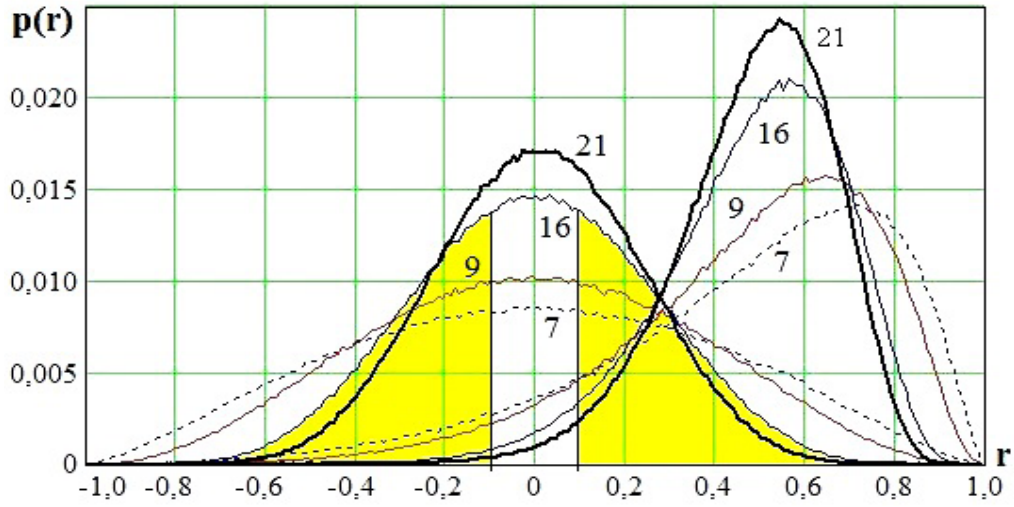
$$r(\nu_i,\nu_m) = \frac{1}{n}\sum_{d=1}^{n}\frac{(E(\nu_i)-\nu_{i,d})\cdot\left(E(\nu_m)-\nu_{m,d}\right)}{\sigma(\nu_i)\cdot\sigma(\nu_m)}. \quad (3)$$

При вычислении коэффициента корреляции происходит накапливание влияния ошибок математических ожиданий $\Delta E(\nu_i)$, $\Delta E(\nu_m)$ и двух стандартных отклонений $\Delta\sigma(\nu_i)$, $\Delta\sigma(\nu_m)$, которые, в свою очередь, зависят от ошибок вычисления математических ожиданий $\Delta\sigma(\nu_i,\Delta E(\nu_i))$, $\Delta\sigma(\nu_m,\Delta E(\nu_m))$.

Таким образом, невозможно точно вычислить коэффициент корреляции на малых выборках. На рис. 1 показано распределение значений коэффициентов корреляции, вычисленных на выборках разного объема.

Из рис. 1 видно, что при выборке из 16 примеров оценка значений независимых данных соответствует коэффициенту корреляции в интервале от –0,7 до +0,7. Если ограничиться значениями, попадающими в интервал от –0,1 до +0,1, то необходимо пропустить порядка 80 % слабо коррелированных параметров. При росте объемов выборки задача вычисления коэффициентов корреляции становится менее сложной, однако невозможно получить большие выборки при обучении преобразователей «Биометрия – код доступа». Пользователи легко идут на предоставление малого количества примеров биометрического образа «Свой». Если требовать от них предъявить большее количество (≤ 21), то пользователи начинают ощущать дискомфорт, рассматривая рост количества примеров в обучающей выборке как ощутимое снижение эргономических качеств их личного средства биометрической аутентификации.

[14] **Ахметов Б. Б., Иванов А. И.** Многомерные статистики существенно зависимых биометрических данных, порождаемые нейросетевыми эмуляторами квадратичных форм : монография. Алматы : LEM, 2016. 86 с.



Р и с. 1. Распределение значений коэффициентов корреляции для выборок из n примеров (n = 7, 9, 16, 21) при двух значениях коэффициентов корреляции: r = 0; r = 0,5

F i g. 1. Distributions of values of correlation coefficients for samples from n = 7, 9, 16, 21 examples with two values of correlation coefficients r = 0 and r = 0,5

Методы и материалы

Известно, что центрированные и нормированные независимые данные попадают в круг рассеивания с заданной вероятностью[15]. При этом для большого количества опытов (N) вероятности попадания в каждую из четвертей круга будут одинаковы:

$$P_1 \approx \frac{n_1}{N} \approx P_2 \approx \frac{n_2}{N} \approx \approx P_3 \approx \frac{n_3}{N} \approx P_4 \approx \frac{n_4}{N}, \quad (4)$$

где n_1, n_2, n_3, n_4 – количество попаданий в первую, вторую, третью и четверную четверти круга соответственно.

В случае, если данные коррелированы, то соотношение между вероятностями попадания в разные фрагменты эллипса рассеивания изменяется:

$$P_1 \approx \frac{n_1}{N} \approx P_3 \approx \frac{n_2}{N} > > P_2 \approx \frac{n_2}{N} \approx P_4 \approx \frac{n_4}{N}. \quad (5)$$

Данная ситуация отражена на рис. 2.

Для коррелированных данных вероятности попадания в эллиптические сектора (рис. 2) пропорциональны малому и большому диаметрам эллипса:

$$\frac{d}{D} = \frac{P_2 + P_4}{P_1 + P_3} \approx \frac{n_2 + n_4}{n_1 + n_3}. \quad (6)$$

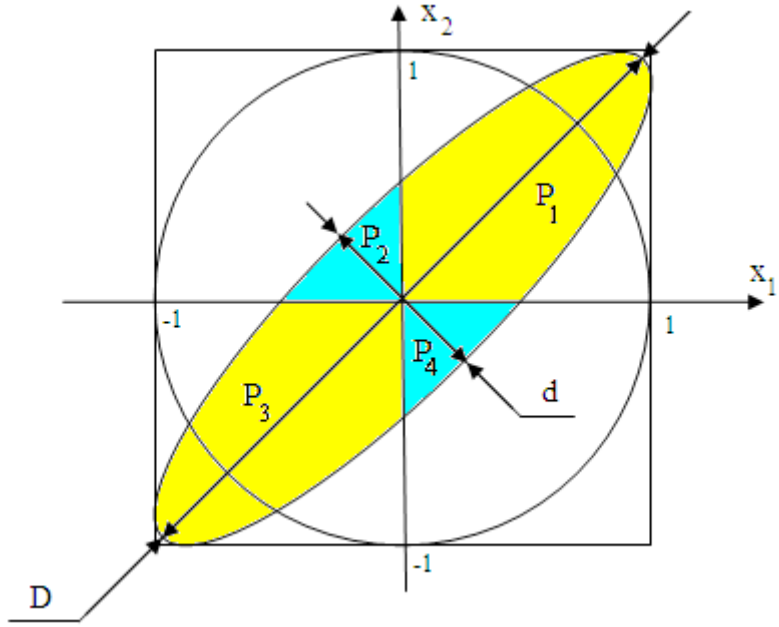
Подставляя соотношение (6) в известную формулу вычисления коэффициента корреляции[15]:

$$r(x_1, x_2) = \frac{D - d}{D + d}, \quad (7)$$

получим формулу для вычисления дискретных значений конечного спектра коэффициентов корреляции:

$$r(x_1, x_2) = \frac{P_1 + P_3 - P_2 - P_4}{P_1 + P_3 + P_2 + P_4} \approx \approx \frac{n_1 + n_3 - n_2 - n_4}{n_1 + n_3 + n_2 + n_4}. \quad (8)$$

[15] **Абезгауз Г. Г.** Справочник по вероятностным расчетам. М. : Воениздат, 1970. 536 с.



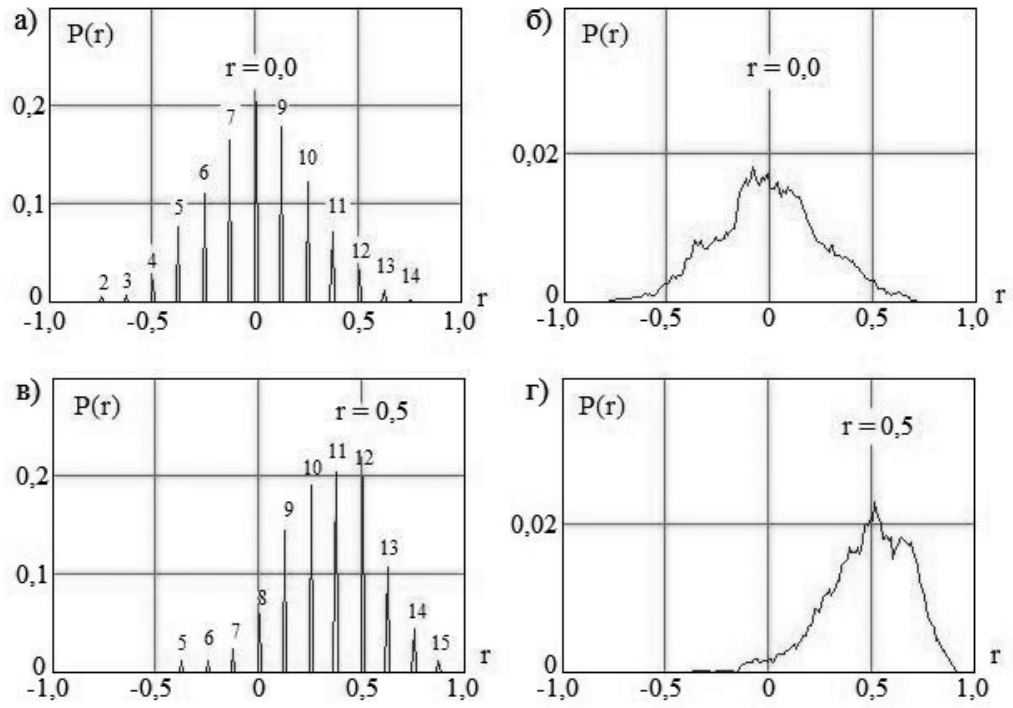
Р и с. 2. Описание центрированных и нормированных площадей рассеивания нормальных данных (независимые данные – круг; зависимые данные – эллипс)

F i g. 2. Description of centered and normalized areas of dispersion of normal data (independent data – circle and dependent data – ellipse)

Таким образом, эллипс распределения зависимых данных является двумерным континуумом корреляционной молекулы, а оси нормированной и центрированной системы координат играют роль двух квантователей, делящих площадь эллипса на четыре части. Получается достаточно простая и понятная математическая конструкция, преобразующая внутренний (не наблюдаемый) двумерный континуум в конечный спектр дискретных выходных состояний. Другими словами, была получена искомая корреляционная молекула, аналогичная хи-квадрат математической молекуле [9–11] или молекуле водорода, состояния которой описываются уравнением Шредингера.

Результаты исследования

Очевидно, что выражение (8) легко может быть воспроизведено программно; более того, два независимых программных генератора псевдослучайных чисел могут быть сцеплены между собой с любым уровнем коррелированности. Далее можно поддерживать как угодно долго работу такого программного генератора, наблюдая на выходе квантовую суперпозицию 15-и дискретных состояний. На рис. 3 приведены два дискретных выходных спектра состояний корреляционной молекулы и распределение значений ее внутреннего континуального состояния обычных коэффициентов корреляции.



Р и с. 3. Примеры дискретного и непрерывного спектров корреляционной молекулы для двух состояний коррелированности внутреннего программного эмулятора двумерного континуума

F i g. 3. Examples of discrete and continuous spectra of the correlation molecule for two states of correlation of the internal software emulator of a two-dimensional continuum

Из рис. 3 видно, что дискретный спектр выходных состояний корреляционной молекулы для выборок из 16 примеров может иметь до 15 спектральных линий, расположенных по отношению к соседям на расстоянии $\Delta r = 0{,}125$. Это позволяет описывать корреляционную молекулу 15-ю членами квантовой суперпозиции:

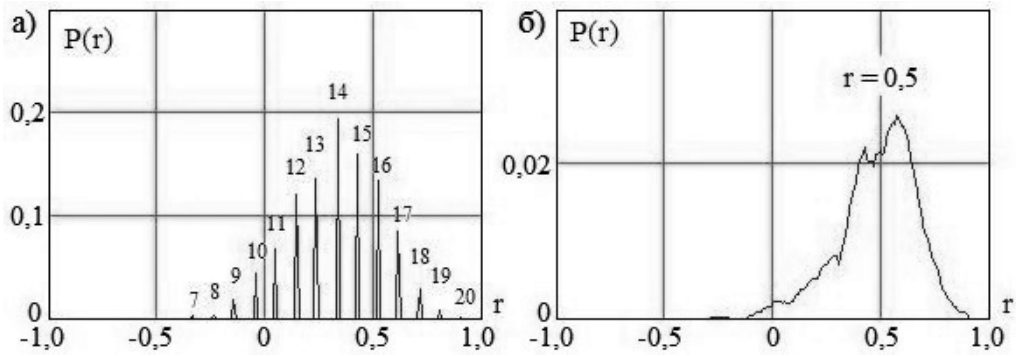
$$|\psi\rangle = \sum_{i=1}^{15} \sqrt{P(r = -1 + 0.125 \cdot i)} \cdot |"bin(i)"\rangle, \quad (9)$$

где "*bin*(*i*)" – бинарная запись индекса в скобках Дирака длиной в 4 кубита.

Следует обратить внимание на отсутствие в квантовой суперпозиции (9) нулевого члена $P(r = -1)$ и последнего 16-го члена $P(r = 1)$ в силу того, что они полностью детерминированы (бесполезны при расчете квантовой сцепленности разрядов 4-кубитного квантового вычислителя).

С помощью индуктивного метода можно показать, что для выборок в 32 опыта количество спектральных линий удвоится, а расстояние между ними уменьшится в два раза до $\Delta r = 0{,}0625$.

Каждой выборке соответствует определенное количество спектральных составляющих и свое расстояние между ними. На рис. 4 показан дискретный спектр состояний корреляционной молекулы для выборки из 21 примера.



Р и с. 4. Дискретный спектр выходных состояний корреляционной молекулы и его непрерывный аналог для выборки, содержащей 21 пример

F i g. 4 Discrete spectrum of the output states of the correlation molecule and its continuous analog for a sample containing 21 examples

Сравнив рис. 3, в–г с рис. 4, нетрудно убедиться в их подобии. Именно на этом подобии может быть построен циклический континуально-квантовый усилитель мощности корреляционного функционала. Подробнее о принципах создания циклических континуально-квантовых усилителей мощности статистических функционалов можно прочесть в работах [10–11], где подсчитано количество циклов под усилитель хи-квадрат критерия для выборки в 21 пример.

Обсуждение и заключения

Попытки описания конструкций перспективных квантовых компьютеров в квантово-механической парадигме Манина-Шредингера сыграли важную роль в создании новой математической теории, однако в прикладном отношении данная парадигма не вносит существенных изменений. Главным препятствием выступает синхронизация квантово-механических «котов Шредингера». Однако данная проблема исчезает, если отказаться от попыток аппаратной реализации уравнений математической физики, построенных под объект микромира – молекулу водорода. Могут быть использованы куда более простые континуально-квантовые программные уравнения математической хи-квадрат молекулы или математической корреляционной молекулы.

При этом не имеет значения, что формального аналитического описания для континуально-квантовых уравнений, построенных для хи-квадрат молекулы и для корреляционной молекулы, не существует. Для прикладной математики аналитические формализации уравнений и их аналитические решения не нужны. Как показано в данной статье, их квантовая суперпозиция содержит от 15 до 20 значимых компонент. Отметим, что их численное моделирование возможно осуществить на обычном компьютере.

Квантовая суперпозиция и квантовая запутанность для корреляционной математической молекулы могут быть представлены не более чем 20-ю описывающими функциям. Данные функции должны совместно использоваться циклическим континуально-квантовым усилителем мощности корреляционного функционала. Объем кода, реализующий такой усилитель, в настоящее время не определен. Однако есть основания полагать, что объем кодов программного усилителя мощности хи-квадрат критерия (хи-квадрат молекулы) и объем кодов усилителя мощности корреляционного функционала

будут сопоставимы. Объем программной реализации квантово-спектрального усилителя мощности корреляционных функционалов предположительно составит до 20 тыс. строк программы на языке высокого уровня. Эта задача не представляет трудностей для группы программистов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Cryptographic key generation from voice / F. Monrose [et al.] // Proc. IEEE Symp. on Security and Privacy. 2001. P. 202–213. URL: https://www.cs.unc.edu/~reiter/papers/2001/SP2.pdf

2. **Ramírez-Ruiz J., Pfeiffer C., Nolazco-Flores J.** Cryptographic keys generation using finger codes // Advances in Artificial Intelligence – IBERAMIA-SBIA 2006 (LNCS 4140). 2006. P. 178–187. URL: http://dl.acm.org/citation.cfm?id=2110882

3. **Hao F., Anderson R., Daugman J.** Crypto with biometrics effectively // IEEE Transactions on Computers. 2006. Vol. 55, no. 9. P. 1073–1074. URL: http://www.cse.msu.edu/~rossarun/BiometricsTextBook/Papers/Security/Hao_IrisBioCrypt_IEEEComputers06.pdf

4. **Иванов А. И.** Нечеткие экстракторы: проблема использования в биометрии и криптографии // Первая миля. 2015. № 1. С. 40–47. URL: http://www.lastmile.su/journal/article/4489

5. **Manin Yu. I.** Classical computing, quantum computing, and Shor's factoring algorithm // Séminaire Bourbaki. 2000. Vol. 1998/99, no. 862. P. 375–404. URL: https://arxiv.org/abs/quant-ph/9903008

6. **Холево А. С.** Классическая и квантовая энтропии как меры информации // Тр. Междунар. науч. конф. «Ситуационные центры и информационно-аналитические системы класса 4i» (г. Москва, 14–16 ноября 2011). Москва-Протвино : Изд-во ИФТИ, 2011, С. 1–5.

7. **Холево А. С.** Гауссовские классически-квантовые каналы: выигрыш от использования сцепленности // Проблемы передачи информации. 2014. Т. 50, вып. 1. С. 3–17. URL: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=ppi&paperid=2129&option_lang=rus

8. The family of chi-square molecules pearson / B. B. Akhmetov [et al.] // Software-Continuum Quantum Accelerators of High-Dimensional Calculations 15th International Conference on Control, Automation and Systems (ICCAS 2015). Busan. URL: http://toc.proceedings.com/28596webtoc.pdf

9. Дискретный характер закона распределения хи-квадрат критерия для малых тестовых выборок / Б. Б. Ахметов [и др.] // Вестник Национальной академии наук Республики Казахстан. 2015. № 1. С. 17–25. URL: http://nauka-nanrk.kz/ru/assets/журнал%202015%201/Вестник_01_2015.pdf

10. Циклические континуально-квантовые вычисления: усиление мощности хи-квадрат критерия на малых выборках / В. П. Кулагин [и др.] // Аналитика. 2016. Т. 30, № 5. С. 22–29. URL: http://www.j-analytics.ru/journal/article/5679

11. Перспективы создания циклической континуально-квантовой хи-квадрат машины для проверки статистических гипотез на малых выборках биометрических данных и данных иной природы / В. И. Волчихин [и др.] // Известия высших учебных заведений. Поволжский регион. Технические науки. 2017. № 1. С. 3–7. URL: http://izvuz_tn.pnzgu.ru/tn117

12. **Manin Yu. I.** Neural codes and homotopy types: mathematical models of place field recognition // Moscow Mathematical Journal. 2015. Vol. 15, no. 4. P. 741–748. URL: http://www.mathjournals.org/mmj/2015-015-004

13. Многомерный статистический анализ биометрических данных сетью частных критериев Пирсона / Б. Б. Ахметов [и др.] // Вестник Национальной академии наук Республики Казахстан. 2015. № 1. С. 5–11. URL: http://nauka-nanrk.kz/ru/assets/журнал%202015%201/Вестник_01_2015.pdf

14. **Волчихин В. И., Ахметов Б. Б., Иванов А. И.** Быстрый алгоритм симметризации корреляционных связей биометрических данных высокой размерности // Известия высших учебных заведений. Поволжский регион. Технические науки. 2016. № 1. С. 3–7. URL: http://izvuz_tn.pnzgu.ru/tn1116

15. Фрактально-корреляционный функционал, используемый при поиске пар слабо зависимых биометрических данных в малых выборках / В. И. Волчихин [и др.] // Вестник высших

учебных заведений. Поволжский регион. Технические науки. 2016. № 4. С. 25–31. URL: http://izvuz_tn.pnzgu.ru/tn3416

16. **Кулагин В. П., Иванов А. И., Серикова Ю. И.** Корректировка методических и случайных составляющих погрешностей вычисления коэффициентов корреляции, возникающих на малых выборках биометрических данных // Информационные технологии. 2016. Т. 22, № 9. С. 705–710. URL: http://novtex.ru/IT/it2016/number09.html

17. **Иванов А. И., Серикова Ю. И.** Номограммы оценки погрешности, коэффициентов корреляции, вычисленных на малых выборках биометрических данных // Вопросы радиоэлектроники. 2015. № 2. С. 123–130.

18. **Иванов А. И., Ложников П. С., Качайкин Е. И.** Идентификация подлинности рукописных автографов сетями Байеса-Хэмминга и сетями квадратичных форм // Вопросы защиты информации. 2015. № 2. С. 28–34.

19. Биометрическая идентификация рукописных образов с использованием корреляционного аналога правила Байеса / А. И. Иванов [и др.] // Вопросы защиты информации. 2015. № 3. С. 48–54.

Поступила 02.03.2017; принята к публикации 05.04.2017; опубликована онлайн 14.06.2017

Об авторах:

Волчихин Владимир Иванович, президент ФГБОУ ВО «Пензенский государственный университет» (440000, Россия, г. Пенза, ул. Красная, д. 40), доктор технических наук, профессор, vvi@pnzgu.ru

Иванов Александр Иванович, начальник лаборатории биометрических и нейросетевых технологий, АО «Пензенский научно-исследовательский электротехнический институт» (440026, Россия, г. Пенза, ул. Советская, д. 9), доктор технических наук, доцент, **ORCID: http://orcid.org/0000-0002-3854-2660**, ivan@pniei.penza.ru

Сериков Андрей Васильевич, начальник отделения АО «Рубин» (440000, Россия, г. Пенза, ул. Байдукова, д. 2), **ORCID: http://orcid.org/0000-0002-6870-3349**, aosv68@bk.ru

Серикова Юлия Игоревна, магистрантка 2-го года обучения кафедры математической обработки и ПЭВМ, ФБГОУ ВО «Пензенский государственный университет» (440000, Россия, г. Пенза, ул. Красная, д. 40), **ORCID: http://orcid.org/0000-0002-4959-321X**, julia-ska@yandex.r

Вклад соавторов: В. И. Волчихин: научное руководство, модернизация квантово-механической парадигмы; А. И. Иванов: формализация требований к многомерным биометрическим данным, формализация требований к объемам тестовых выборок; А. В. Сериков: синтез механизма квантования двухмерного континуума внутренних состояний корреляционной молекулы; Ю. И. Серикова: программная реализация, вычисление положения и амплитуды спектральных линий.

Все авторы прочитали и одобрили окончательный вариант рукописи.

REFERENCES

1. Monroes F., Reiter M. K., Li Q., Wetzel S. Cryptographic key generation from voice. In: Proc. IEEE Symp. on Security and Privacy. 2001. p. 202-213. Available at: https://www.cs.unc.edu/~reiter/papers/2001/SP2.pdf

2. Ramírez-Ruiz J., Pfeiffer C., Nolazco-Flores J. Cryptographic keys generation using FingerCodes. In: Advances in Artificial Intelligence – IBERAMIA-SBIA 2006 (LNCS 4140). 2006; 178-187. Available at: http://dl.acm.org/citation.cfm?id=2110882

3. Hao F., Anderson R., Daugman J. Crypto with biometrics effectively. IEEE Transactions on Computers. 2006; 9(55):1073-1074. Available at: http://www.cse.msu.edu/~rossarun/BiometricsTextBook/Papers/Security/Hao_IrisBioCrypt_IEEEComputers06.pdf

4. Ivanov A. I. [Fuzzy extractors: A problem of use in biometrics and cryptography]. *Pervaya milya* = First mile. 2015; 1:40-47. Available at: http://www.lastmile.su/journal/article/4489 (In Russ.)

5. Manin Yu. I. Classical computing, quantum computing, and Shor's factoring algorithm. Séminaire Bourbaki. 2000; 862:375-404. Available at: https://arxiv.org/abs/quant-ph/9903008

6. Kholevo A. S. [Classical and quantum entropies as measures of information]. In: *Trudy Mezhdunarodnoy nauchnoy konferentsii "Situatsionnyye tsentry i informatsionno-analiticheskiye sistemy klassa 4i"* [Situational centers and information-analytical systems of 4i class: Proceedings]. Moscow: IFTI Publ; 2011; 1-5.

7. Kholevo A. S. On the gain of entanglement assistance in the classical capacity of quantum gaussian channels. *Problemy peredachi informatsii* = Problems of Information Transfer. 2014; 1(50):3-17. Available at: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=ppi&paperid=2129&option_lang=rus (In Russ.)

8. Akhmetov B., Ivanov A., Gilmutdinov A., Bezyayev A., Funtikova Yu. The family of chi-square molecules pearson. In: Software-Continuum Quantum Accelerators of High-Dimensional Calculations 15th International Conference on Control, Automation and Systems (ICCAS 2015). Pusan; 2015; 1337-1341. Available at: http://toc.proceedings.com/28596webtoc.pdf

9. Akhmetov B. B., Ivanov A. I., Serikova N. I., Funtikova Yu. V. Discrete character of the law of chi-square distribution criterion for small test selections of values. *Vestnik Natsionalnoy akademii nauk Respubliki Kazakhstan* = The Bulletin of the National Academy of Sciences of the Republic of Kazakhstan. 2015; 1:17-25. Available at: http://nauka-nanrk.kz/ru/assets/журнал%202015%201/Вестник_01_2015.pdf (In Russ.)

10. Kulagin V., Ivanov A., Gazin A., Akhmetov B. [Cyclic continuum-quantum computing: Strengthening the chi-square power of a criterion on small samples]. *Analitika* = Analytics. 2016; 5(30):22-29. Available at: http://www.j-analytics.ru/journal/article/5679 (In Russ.)

11. Volchikhin V. I., Ivanov A. I., Pashchenko D. V., Akhmetov B. B., Vyatchanin S. Ye. [Prospect of creating a cyclic continual-quantum chi-square machine for testing statistical hypotheses on small test samples of biometric data and data of a different nature]. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskiye nauki* = Higher Education Bulletin. Volga region. Technical science. 2017; 1:3-7. Available at: http://izvuz_tn.pnzgu.ru/tn117 (In Russ.)

12. Manin Yu. I. Neural codes and homotopy types: mathematical models of place field recognition. *Moskovskiy matematicheskiy zhurnal* = Moscow Mathematical Journal. 2015; 4(15):741-748 Available at: http://www.mathjournals.org/mmj/2015-015-004 (In Russ.)

13. Akhmetov B. B., Ivanov A. I., Bezyayev A. V., Funtikova Yu. V. Multidimensional statistical analysis of biometric data by network of private Pearson's criteria. *Vestnik Natsionalnoy akademii nauk Respubliki Kazakhstan* = The Bulletin of the National Academy of Sciences of the Republic of Kazakhstan. 2015; 1:5-11. Available at: http://nauka-nanrk.kz/ru/assets/журнал%202015%201/Вестник_01_2015.pdf (In Russ.)

14. Volchikhin V. I., Akhmetov B. B., Ivanov A. I. [A fast symmetrization algorithm for correlations of biometric data of high dimension]. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskiye nauki* = Higher Education Bulletin. Volga region. Technical science. 2016. 1:3-7 Available at: http://izvuz_tn.pnzgu.ru/tn1116 (In Russ.)

15. Volchikhin V. I., et al. [Fractal-correlation functional used in the search for pairs of weakly dependent biometric data in small samples]. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskiye nauki* = Higher Education Bulletin. Volga region. Technical science. 2016; 4:25-31. Available at: http://izvuz_tn.pnzgu.ru/tn3416 (In Russ.)

16. Kulagin V. P., Ivanov A. I., Serikova Yu. I. [Correction of methodological and random components of errors in the calculation of correlation coefficients arising on small samples of biometric data]. *Informatsionnyye tekhnologii* = Information Technology. 2016; 9(22):705-710. Available at: http://novtex.ru/IT/it2016/number09.html (In Russ.)

17. Ivanov A. I., Serikova Yu. I. [Nomograms of error estimation, correlation coefficients calculated on small samples of biometric data]. *Voprosy radioelektroniki* = Problems of Radio and Electronics. 2015; 2:123-130. (In Russ.)

18. Ivanov A. I., Lozhnikov P. S., Kachaykin Ye. I. [Identification of authenticity of handwritten autographs by Bayes-Hamming networks and networks of quadratic forms]. *Voprosy zashchity informatsii* = Information Security Problems. 2015; 2:28-34. (In Russ.)

19. Ivanov A. I., Kachaykin Ye. I. Lozhnikov P. S., Sulavko A. Ye. [Biometric identification of handwritten images using the correlation analogue of the Bayes' rule]. *Voprosy zashchity informatsii* = Information Security Problems. 2015; 3:48-54. (In Russ.)

Submitted 02.03.2017; revised 05.04.2017; published online 14.06.2017

About the authors:

Vladimir I. Volchikhin, President of the Penza State University (40 Krasnaya St., Penza 440000 Russia), Dr.Sci. (Engineering), professor, vvi@pnzgu.ru

Aleksandr I. Ivanov, Head of the Laboratory of Biometric and Neural Network Technologies, Penza Electrotechnical Research Institute (9 Sovetskaya St., Penza 440026, Russia), Dr.Sci. (Engineering), docent, **ORCID: http://orcid.org/0000-0002-3854-2660**, ivan@pniei.penza.ru

Andrey V. Serikov, Head of Department of Joint-Stock Company Rubin (2 Baydukova St., Penza 440000, Russia), **ORCID: http://orcid.org/0000-0002-6870-3349**, aosv68@bk.ru

Yuliya I. Serikova, Graduate Student of the Penza State University (40 Krasnaya St., Penza 440000 Russia), **ORCID: http://orcid.org/0000-0002-4959-321X**, julia-ska@yandex.r

Contribution of the co-authors: V. Volchikhin: scientific supervision, modernization of the quantum-mechanical paradigm; A. Ivanov: formalization of requirements for multidimensional biometric data, formalization of requirements for the volume of test samples; A. Serikov: synthesis of the mechanism of quantization of the two-dimensional continuum of internal states of the correlation molecule; Yu. Serikova: software implementation, calculation of position and amplitude of spectral lines.

All authors have read and approved the final version of the manuscript.