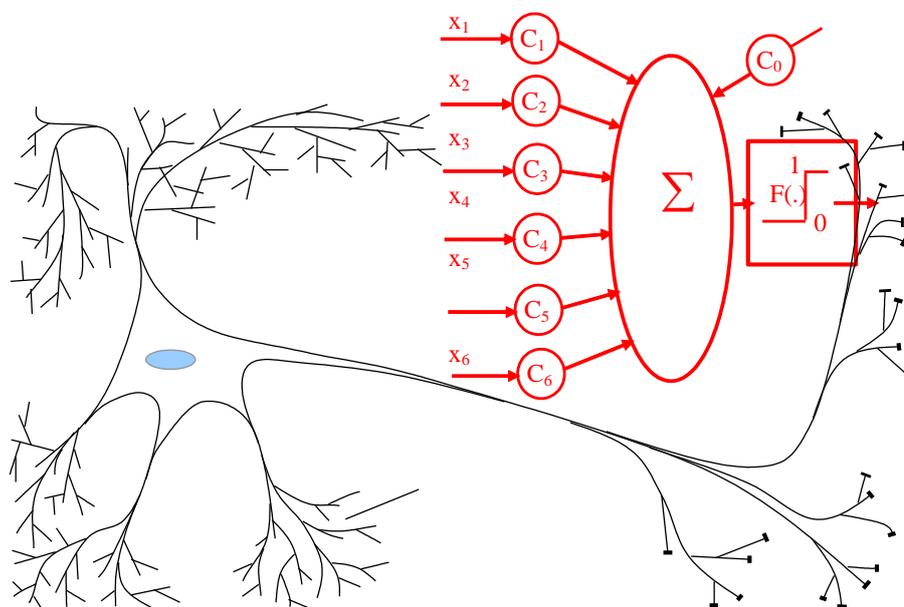


МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Пензенский государственный университет» (ПГУ)

А. И. Иванов

НЕЙРОДИНАМИКА: ГИПЕРУСКОРЕНИЕ
НАПРАВЛЕННЫХ ПЕРЕБОРОВ ИЛИ ПОВЫШЕНИЕ
ДОСТОВЕРНОСТИ СТАТИСТИЧЕСКИХ ОЦЕНОК
НА МАЛЫХ ВЫБОРКАХ

Препринт



Пенза
Издательство ПГУ
2021

УДК 519.24; 53; 57.017

ББК 32.818

И20

Р е ц е н з е н т ы :

доктор технических наук, профессор,
заведующий кафедрой «Компьютерные технологии»
Пензенского государственного университета
В. И. Горбаченко;

доктор технических наук, профессор,
ученый секретарь научно-технического совета
научно-производственного предприятия «Рубин» (г. Пенза)
М. М. Бутаев

Иванов, Александр Иванович.

И20

НейроДинамика: гиперускорение направленных переборов или повышение достоверности статистических оценок на малых выборках : препринт / А. И. Иванов. – Пенза : Изд-во ПГУ, 2021. – 106 с.

ISBN 978-5-907456-70-9

Большие сети искусственных нейронов обычно используются в статическом режиме. Статика применения нейронных сетей понятна и хорошо исследована, однако в статическом режиме НейроПроцессоры оказываются не способными давать огромные ускорения при решении задач направленного перебора. Еще одним важным недостатком является то, что нейросети в статике не могут принимать решения высокой достоверности при анализе малых выборок. Нет живых существ, чьи естественные нейроны работали бы в НейроСтатике. Люди умны только потому, что их естественные нейроны решают свои задачи в динамике.

Рассматривается решение ряда задач, для которых перевод искусственных нейронных сетей из статике в динамику дает огромные преимущества. То, что сегодня принято называть «сильным» искусственным интеллектом, скорее всего, технически можно реализовать только в НейроДинамике.

Издание ориентировано на студентов, аспирантов, преподавателей, инженеров, занимающихся проблемами применения НейроСетевого искусственного интеллекта для решения задач биометрии и иных приложений искусственного интеллекта.

УДК 519.24; 53; 57.017
ББК 32.818

ISBN 978-5-907456-70-9

© Иванов А. И., 2021

СОДЕРЖАНИЕ

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ	6
ВВЕДЕНИЕ.....	8
ГЛАВА ПЕРВАЯ. АВТОМАТИЧЕСКОЕ ОБУЧЕНИЕ СЕТЕЙ ИСКУССТВЕННЫХ НЕЙРОНОВ И ТЕСТИРОВАНИЕ КАЧЕСТВА ИХ РАБОТЫ.....	14
1.1. Искусственные нейроны, накапливающие (обогащающие) входные данные в многомерных линейных и нелинейных пространствах	14
1.2. Персептроны – искусственные нейроны с накоплением данных в линейном многомерном пространстве.....	16
1.3. Автоматическое обучение нейронов с накоплением данных в многомерном линейном пространстве.....	17
1.4. Экономия памяти и сокращение времени при тестировании обученной нейросети на малых выборках в пространстве расстояний Хэмминга.....	20
1.5. Экономия памяти и сокращение времени при тестировании обученной НейроСети на малых выборках в пространстве корреляционной сцепленности разрядов длинных кодов.....	23
ГЛАВА ВТОРАЯ. ГИПЕРУСКОРЕНИЕ ПЕРЕБОРА ОБРАЗОВ «ЧУЖОЙ» ПРИ ИЗВЛЕЧЕНИИ ЗНАНИЙ ИЗ ТАБЛИЦ ОБУЧЕННОЙ СЕТИ ПЕРСЕПТРОНОВ.....	27
2.1. Извлечение знаний из НейроСетевого преобразователя биометрия-код путем направленного синтеза образов «Чужой» с монотонно уменьшающейся энтропией.....	27
2.2. Оценка достижимого гиперускорения выполнения направленного перебора при переходе от анализа данных в НейроСтатике к анализу данных в НейроДинамике	31
2.3. БИОНИКА – копирование естественных НейроСетевых структур людей и других живых существ, непрерывно находящихся в динамике и имеющих внутренние механизмы многоуровневого квантования.....	34
2.4. Квантовые процессоры как перспектива совершенствования машин фон Неймана в период с 1980 по 2011 г.	38
2.5. Неопределенность Гейзенберга для НейроДинамики (либо ускорение вычислений, либо повышение их достоверности)	41
ГЛАВА ТРЕТЬЯ. НЕЙРОСЕТЕВОЕ ОБОБЩЕНИЕ НЕСКОЛЬКИХ СТАТИСТИЧЕСКИХ КРИТЕРИЕВ ПРОВЕРКИ ГИПОТЕЗЫ НОРМАЛЬНОГО РАСПРЕДЕЛЕНИЯ МАЛЫХ ВЫБОРОК В НЕЙРОСТАТИКЕ.....	46
3.1. НейроСетевое обобщение классического критерия хи-квадрат (1900 г.) и критерия Крамера – фон Мизеса (1928 г.)	46

3.2. Нейросетевое обобщение классического критерия Смирнова – Крамера – фон Мизеса (1936 г.), Андерсона – Дарлинга (1952 г.) и критерия Фроцини (1978 г.).....	48
3.3. НейроКритерии Муроты – Такеучи (1981 г.) и Васичека (1976 г.).....	50
3.4. Сеть из 21 искусственного нейрона, полученных обобщением 21 классического статистического критерия	52
3.5. Симметризация НейроСетевых обобщений статистических критериев для учета значений их коэффициентов взаимной корреляции	54
ГЛАВА ЧЕТВЕРТАЯ. ПЕРЕХОД ИЗ НЕЙРОСТАТИКИ В НЕЙРОДИНАМИКУ, ЗАМЕНА СТАТИСТИЧЕСКИХ НЕЙРОКРИТЕРИЕВ МАТЕМАТИЧЕСКИМИ МОЛЕКУЛАМИ	58
4.1. Наблюдение спектра амплитуд вероятности появления расстояний Хэмминга путем модуляции входных данных НейроСети через их случайное прореживание	58
4.2. Математическая хи-квадрат молекула.....	61
4.3. Интеллектуализация автоматического алгоритма обучения сетей искусственных нейронов на малых обучающих выборках	66
4.3.1. НейроСетевое предсказание ошибок вычисления математического ожидания и стандартного отклонения на малых выборках с нормальным распределением данных	66
4.3.2. НейроСетевая интеллектуализация автоматического алгоритма обучения сетей корреляционных нейронов Байеса	71
4.4. Необходимость компенсации блужданий, возникающих при попытках вычислений младших статистических моментов на больших выборках	75
ЗАКЛЮЧЕНИЕ	78
СПИСОК ЛИТЕРАТУРЫ.....	80
Приложение 1. Численное моделирование шести статистических критериев для проверки гипотезы нормального распределения выборок, объемом по 16 опытов (KfM – Крамера – фон Мизеса; χ^2 ; SKfM – Смирнова – Крамера – фон Мизеса; AD – Андерсона – Дарлинга; F – Фроцини; MT – Муроты – Такеучи; V – Васичека)	90
Приложение 2. Моделирование кодовых откликов в пространстве расстояний Хэмминга симметричных сетей искусственных нейронов с 16 выходами.....	94
Приложение 3. Формирование колоды из 64 карт случайным отбрасыванием по 5 опытов из первоначальной избыточной выборки в 21 опыт.....	96
Приложение 4. Численное моделирование дискретной хи-квадрат молекулы Пирсона для малых выборок из 16 опытов с нормальным и равномерным распределением	98

Приложение 5. Ошибки вычисления математических ожиданий и стандартных отклонений из-за ограниченных малых выборок обучения ...	100
Приложение 6. Ошибки вычисления коэффициентов корреляции из-за ограниченных малых выборок обучения	101
Приложение 7. Пример блуждания, возникающих при вычислении математического ожидания и стандартного отклонения на большой выборке в 1000 опытов	102
Список ранее опубликованной литературы издательствами «Пензенского научно-исследовательского электротехнического института» и «Пензенского государственного университета» по близкой тематике	103

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ

Автомат обучения НейроСети – автомат, выполняющий обучение НейроСети, являющийся устойчивым и позволяющий за заданный интервал времени обучить большую сеть искусственных нейронов на заданной большой или малой обучающей выборки.

«БиоНейроАвтограф» – общедоступное, свободно используемое программное обеспечение, позволяющее получать большие объемы достоверной биометрической информации в учебных целях (например, для выполнения лабораторных работ).

БиоАПИ – международный стандарт, описывающий программный интерфейс приложений при взаимодействии между аппаратными фрагментами биометрических систем.

БиоШаблон – вектор биометрических данных, являющихся шаблоном простейшего решающего правила, например, в форме математических ожиданий биометрических параметров и интервалы их допустимых отклонений.

БиоПараметр – биометрический параметр получаемый вычислением из данных биометрического образа человека.

Биометрический образ – связанные между собой данные, полученные сканированием реальных данных с реальных датчиков.

Искусственный нейрон – любая математическая конструкция, построенная для воспроизведения вычислительных эффектов, наблюдаемых у естественных нейронов людей и иных живых существ (бионика).

НейроДинамика – описание и использование искусственных нейронов в динамике (на входы нейрона или НейроСети подаются вектора входных данных, на выходе нейрона или нейросети появляются вектора выходных состояний).

НейроКритерий – искусственный нейрон, воспроизводящий тот или иной статистический критерий.

НейроСтатика – описание и использование искусственных нейронов в статике (на входы нейрона или НейроСети подаются вектор входных данных, на выходе нейрона или нейросети появляется один отклик).

Сеть искусственных нейронов – объединение множества искусственных нейронов, выполняющих параллельное и последовательное вычисление данных.

c_i – i -тый разряд кода «Свой», состоящего из 256 разрядов в среде моделирования «БиоНейроАвтограф».

v_i – i -тый БиоПараметр образа «Свой», состоящего из 416 БиоПараметров в среде моделирования «БиоНейроАвтограф».

x_i – i -тый разряд кода «Чужой», состоящего из 256 разрядов в среде моделирования «БиоНейроАвтограф».

ξ_i – i -тый БиоПараметр образов «Чужой», состоящего из 416 БиоПараметров в среде моделирования «БиоНейроАвтограф».

ВВЕДЕНИЕ

Развитие приложений искусственного интеллекта сегодня идет стремительно (экспоненциально). Одним из направлений развития является стандартизация разработки приложений искусственного интеллекта. Эта тенденция хорошо наблюдаема на примерах биометрических технологий. Для ускорения темпов развития в 2002 г. был создан международный комитет по стандартизации ISO/IEC JTC1 sc37 (Биометрия). С момента своего создания этот технический комитет уже разработал и имеет на этапе разработки 174 стандарта. Разрабатывается и вводится в действие примерно по 6–7 биометрических стандартов в год. Биометрия оказалась лидером по стандартизации неслучайно. Биометрические технологии, видимо, должны стать основой личной безопасности людей в будущем. Поддержка безопасности своих граждан – это компетенция каждого из современных государств. В связи с этим параллельно с международными стандартами должны существовать и национальные стандарты, опирающиеся на национальную биометрию и национальную криптографию. На настоящий момент в России активно развивается нейросетевая биометрия, регламентируемая 8 национальными стандартами.

НейроСетевую биометрию следует рассматривать как некоторую часть искусственного интеллекта, развивающуюся с учетом применения базовых правил обеспечения информационной безопасности. Далеко не любое решающее правило искусственного интеллекта может быть надежно защищено, например, путем шифрования его компонент. В этом отношении нейросетевые решающие правила оказываются выгодными в контексте использования, вроде бы, универсальной гомоморфной криптографии.

Следует отметить, что первая достаточно универсальная спецификация взаимодействия биометрических сканеров с вычислителями –

БиоАПИ, создавалась как национальный стандарт США в 1996–1998 г. Уже тогда была понятна проблема безопасного сопряжения биометрии (биометрических шаблонов) и криптографии. Если интернет-холодильник будет узнавать «Своего» хозяина по его лицу или голосу, а хозяин будет дорожить своей интернет-репутацией, то защищать свою репутацию придется криптографией. В соответствии с БиоАПИ БиоШаблоны придется шифровать, но тогда ими уже нельзя пользоваться. Перед каждым применением БиоШаблона его придется расшифровывать, т.е. рядом с БиоШаблоном в программном обеспечении интернет-холодильника придется почти открыто хранить криптографический ключ. Хранить ключ «под ковриком» рядом с хорошо защищенной полноценной криптографией «дверью» опасно.

Опасно хранить ключ «под ковриком» не потому, что злоумышленник истратит ресурсы интернет-кошелька вашего интернет-холодильника, заполнив его пивом или колбасой одного рекламодателя. Значительные репутационные потери для владельца интернет-холодильника могут возникнуть, если сторонний злоумышленник заставит ваш интернет-холодильник или ваш интернет-телевизор с вашего IP-адреса участвовать в DOS-атаке на портал Госуслуг или иной государственный портал.

Если ваша собака, находясь без намордника, покусала представителя власти или соседку, то отвечать придется вам лично. Переложить ответственность на производителя вашего интернет-холодильника, вашего интернет-телевизора или заводчика, продавшего вам щенка, не получится.

В конце прошлого века предполагалось, что вот-вот появится гомоморфная криптография и решит проблему хранения ключа «под ковриком». Гомоморфно зашифрованные данные можно обрабатывать без их расшифровывания. Однако, первый стандарт по гомоморфному шиф-

рованию ISO/IEC 18033-6:2019 появился только через 20 лет. Причем этот стандарт обеспечивает гомоморфизм только для двух типов операций: операций сложения и операций умножения. При этом практика применения стандарта выявила у схем гомоморфного шифрования серьезный недостаток: они накапливают ошибки. Простые решающие правила с 4 операциями сложения и 4 операциями умножения вполне работоспособны. Однако, если число операций сложения и умножения увеличить до 16, 32, 64, то итоговый шифротекст решающего правила перестает однозначно расшифровываться. Вероятным становится неверное расшифровывание результатов вычисления. Заметим, что для обычных средств шифрования объем защищаемых данных может быть как угодно велик. Обычное шифрование не накапливает ошибок округления.

В этом отношении активно развиваемые в России НейроСетевые технологии обработки биометрических данных ослабляют требования по минимальной сложности решающих правил искусственного интеллекта. Большую сеть искусственных нейронов, требующую для ее реализации десятки тысяч операций сложения и умножения, всегда можно упростить до 4–8 операций сложения и умножения, достаточных для реализации одного нейрона. Было бы идеальным, если бы в ближайшем будущем удалось расширить возможности гомоморфного шифрования, добавив к двум операциям сложения и умножения третью операцию – сравнения с зашифрованным порогом. Тогда отдельные искусственные нейроны и сети из них легко могут быть защищены следующим поколением схем гомоморфного шифрования.

Следует отметить, что НейроСети, созданные для нейросетевой отечественной биометрии, существенно отличаются от своих иностранных аналогов. Главное требование информационной безопасности – это сохранение в тайне биометрического образа и связанного с ним НейроСетью личного криптографического ключа пользователя. В связи

с этим обучение нейронных сетей должно быть полностью автоматическим и должно выполняться на малой выборке в 20 примеров образа «Свой». После обучения криптографический ключ и примеры образа «Свой» должны быть удалены из средства защиты. Если средство защиты физически попадает в руки злоумышленников, то извлечь биометрию пользователя и его криптографический ключ оказывается технически невозможно.

Одним из элементов защиты биометрии пользователя и его криптографического ключа является использование доверенной вычислительной среды, например, процессора SIM-карты, процессора microSD-карты, процессора кредитной карты, процессора карты с RFID считыванием данных. Доверенная вычислительная среда может быть выполнена в виде USB-токена (брелока) или Wi-Fi-токена (брелока). В этом случае злоумышленник не может видеть параметры НейроСети, автоматически обученной по ГОСТ Р 52633.5–2011. При этом возникает иллюзия, что, разместив НейроСетевой процессор в доверенную вычислительную среду, мы полностью решаем задачу информационной безопасности без криптографии.

Такая точка зрения была популярна среди специалистов до 2009 г., когда была написана первая в мировой практике машина, извлекающая знания из обученной нейронной сети. Фактически эта машина опиралась на использование базы из 10000 образов «Чужой» и строилась на автоматической подстановке данных образов «Чужой» на входы исследуемой НейроСети. Исходная небольшая тестовая база в 10000 естественных образов «Чужой» быстро заканчивалась, однако ее оказалось достаточно для поиска 50 наиболее близких образов «Чужой» к образу «Свой». Образ «Свой» обладает практически нулевой энтропией выходных кодов (это результат обучения), т.е. при извлечении знаний нам необходимо выбирать 50 образов «Чужой» с наименьшей энтропией.

Далее нужно воспроизводить процессы природной эволюции. Для извлечения знаний приходится скрещивать 50 образов-родителей между собой и получать от них образы-потомки (процедура скрещивание описана в ГОСТ Р 52633.2–2010). Скрещивание выполняется до восстановления исходной численности в 10000 образов «Чужой».

При повторении процедуры отбора и восстановления численности образов в следующих поколениях удастся все ближе и ближе подобраться к неизвестному образу «Свой». При примерно 50 поколениях искусственной эволюции удастся восстановить неизвестные биометрические параметры образа «Свой» с доверительной вероятностью 0,97. Также удастся восстановить 97 % бит личного криптографического ключа «Свой».

В итоге получается, что за десятки минут на обычном компьютере удастся решить обратную задачу нейросетевой биометрии. Фактически удастся обращать любую матрицу НейроСетевых функционалов размерности 416×256 . Это неожиданно для обычной линейной алгебры, где проблема плохой обусловленности (плохой обращаемости) возникает даже для матриц относительно малой размерности 16×16 .

Анализ причин наблюдаемого эффекта обращения матриц высокой размерности показал, что он обусловлен двумя причинами. Во-первых, нейросетевые функционалы действительно дают более устойчивые решения в сравнении с классикой. Во-вторых, все нейросетевые машины оказываются очень эффективны, если внутри них программно поддерживаются изменения входных состояний искусственных нейронов. Формально происходит отказ от использования нейросетей в статике и переход к поддержке работы НейроСетей в режиме НейроДинамики.

Именно создание больших нейросетевых машин, работающих в динамике, видимо, станет в ближайшее время вектором бурного развития нейросетевых приложений искусственного интеллекта. Люди явля-

ются умными только потому, что наши естественные нейроны не могут находиться в статике. НейроДинамика позволяет либо многократно ускорить вычисления, либо многократно повысить достоверность принимаемых НейроСетевыми процессорами решений.

В данной книге мы попытались рассмотреть математические причины, по которым удастся получить огромные ускорения или огромное повышение достоверность статистических оценок на малых выборках. Естественно, что многие эффекты НейроДинамики не имеют сегодня аналитического описания (корректного математического обоснования). Причиной этого, прежде всего, является высокая размерность решаемых НейроСетями задач. В этом контексте в ближайшее время должен произойти рост размерности задач, решаемых приложениями искусственного интеллекта.

ГЛАВА ПЕРВАЯ

АВТОМАТИЧЕСКОЕ ОБУЧЕНИЕ СЕТЕЙ ИСКУССТВЕННЫХ НЕЙРОНОВ И ТЕСТИРОВАНИЕ КАЧЕСТВА ИХ РАБОТЫ

1.1. Искусственные нейроны, накапливающие (обогащающие) входные данные в многомерных линейных и нелинейных пространствах

Первая работа по искусственным нейронам появилась в 1943 г. [1], т.е. НейроСетевая обработка возникла практически одновременно с ламповыми ЭВМ Тьюринга в «Блетчли парке» [2]. НейроСетевые процессоры и дискретные процессоры Тьюринга параллельно развивались 80 лет. Сегодня мы видим практически полную победу дискретных процессоров над непрерывными НейроСетевыми процессорами. Дискретные вычислители достаточно быстро прошли этапы развития от очень больших ламповых машин до малогабаритных малопотребляющих микропроцессоров, встраиваемых в наручные часы.

Нейронные процессоры развивались куда более драматично [3], проходя через спады и подъемы интереса к ним. Схемы реализации трех типов простейших нейронов приведены на рис. 1.

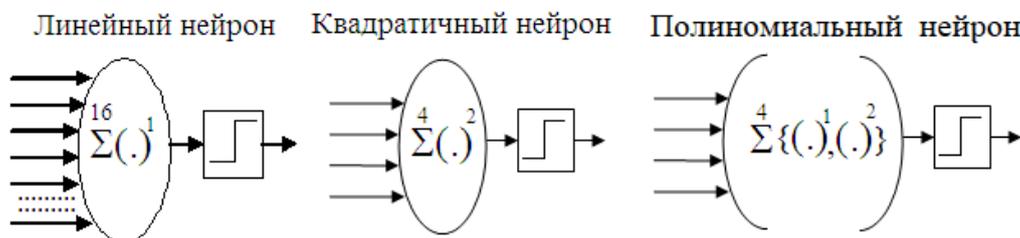


Рис. 1. Простейшие линейный, квадратичный и полиномиальный нейроны

Из рисунка видно, что «сырые» входные данные искусственных нейронов поступают на сумматор, который их накапливает (обогащает)

до некоторого приемлемого для принятия решений качества. Далее выполняется квантование данных. Хорошо изучены линейные и квадратичные нейроны, выполняющие взвешенное накопление данных, соответственно, в линейных и квадратичных пространствах. Проведя еще одно взвешивание каждого из суммируемых элементов, мы можем объединить линейное и квадратичное деформирование пространств накопления данных. В этом случае мы получим более сложный и менее изученный тип полиномиальных нейронов. Для нас важно то, что входной элемент всех искусственных нейронов выполняет обогащение входных «сырых» данных, а выходной пороговый элемент нейронов выполняет квантование уже обогащенных данных.

Обогащение входных «сырых» данных выполняется их взвешенным накапливанием (суммированием), весовые коэффициенты обычно подбираются или вычисляются при обучении нейрона. Чем хуже качество входных данных, тем больше входов должен иметь искусственный нейрон (искусственный обогатитель).

Заметим, что существует несколько сотен алгоритмов обучения искусственных нейронов [3]. В основном все известные алгоритмы обучения нейронов являются итерационными. Для них нет гарантии, что обучение будет выполнено за приемлемое время и что качество обучения будет достаточно высоким. В этом отношении нас будут интересовать только неитерационные алгоритмы обучения. Первый стандартизованный неитерационный алгоритм появился в России – ГОСТ Р 52633.5–2011 [4]. Он описывает автомат обучения для нейронов с линейным накоплением данных. Видимо, следующим стандартизованным алгоритмом будет аналог первого алгоритма для квадратичных нейронов [5]. Третий алгоритм с высокой вероятностью также будет отечественным [6] и будет касаться больших сетей корреляционных нейронов Байеса. Последним должен появиться стандартизованный отечественный

алгоритм для автоматического обучения сетей полиномиальных ортогональных нейронов [7].

1.2. Персептроны – искусственные нейроны с накоплением данных в линейном многомерном пространстве

Рассмотрим простейшие нейроны с линейным накоплением данных (персептроны) [3]. Входные данные персептрона непрерывные (континуальные), а отклик персептрона дискретен и может принимать два состояния «0» или «1»:

$$\left\{ \begin{array}{l} y \leftarrow \sum_{i=1}^{16} \mu_i \cdot x_i \\ z(y) \leftarrow "0" \quad \text{if } z(y) < k. \\ z(y) \leftarrow "1" \quad \text{if } z(y) \geq k \end{array} \right. \quad (1)$$

Настройка или обучение нейрона обычно выполняется подбором или вычислением значений весовых коэффициентов сумматора, а также вычислением (подбором) порога квантователя. Меняя весовые коэффициенты μ_i и значения порога квантователя – k , можно добиться того, чтобы персептрон стал способен распознавать два класса, если они линейно разделимы.

Число входов у искусственного нейрона должно обеспечивать его способность обогащать входные данные до нужного уровня информативности. Так в среде моделирования «БиоНейроАвтограф» [8, 9] используются нейроны с 24 входами. Столь значительное число входов обусловлено ориентацией этого программного продукта на плохие биометрические данные, полученные при рукописном воспроизведении студентами одиночных букв и знаков манипулятором «мышь».

Если бы этот программный продукт был ориентирован только на ввод данных с графического планшета или с чувствительного экрана

ноутбука, то искусственные нейроны могли бы иметь по 16 входов, что отражено в формуле (1). Биометрические данные в этом случае имеют более высокую информативность (более высокое качество). Чем выше качество входных данных, тем меньше нужно входов у входных сумматоров персептронов.

1.3. Автоматическое обучение нейронов с накоплением данных в многомерном линейном пространстве

Одним из важных преимуществ персептронов в биометрических приложениях является то, что их автоматическое обучение регламентируется национальным стандартом ГОСТ Р 52633.5 [4]. По этому стандарту при синтезе структурных связей НейроСетевого преобразователя биометрия-код входы каждого из нейронов случайно подключаются к вектору входных биометрических данных. На рис. 2 приведен пример реализации случайного подключения входов нейронов к входным биометрическим данным.

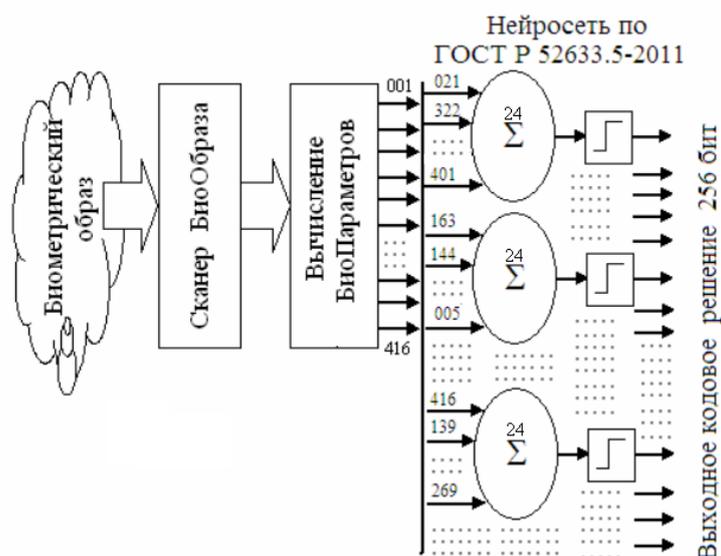


Рис. 2. Пример реализации НейроСети со случайным подключением входов каждого из 256 искусственных нейронов к входным биометрическим данным (среда моделирования «БиоНейроАвтограф» [4])

Так как стандарт ориентирован на приложения информационной безопасности, все пороги квантователей его нейронов одинаковы и соответствуют математическому ожиданию выходных состояний сумматоров нейронов при воздействии на нейросеть алфавитом возможных образов «Чужие». Эта ситуация отображена на рис. 3.

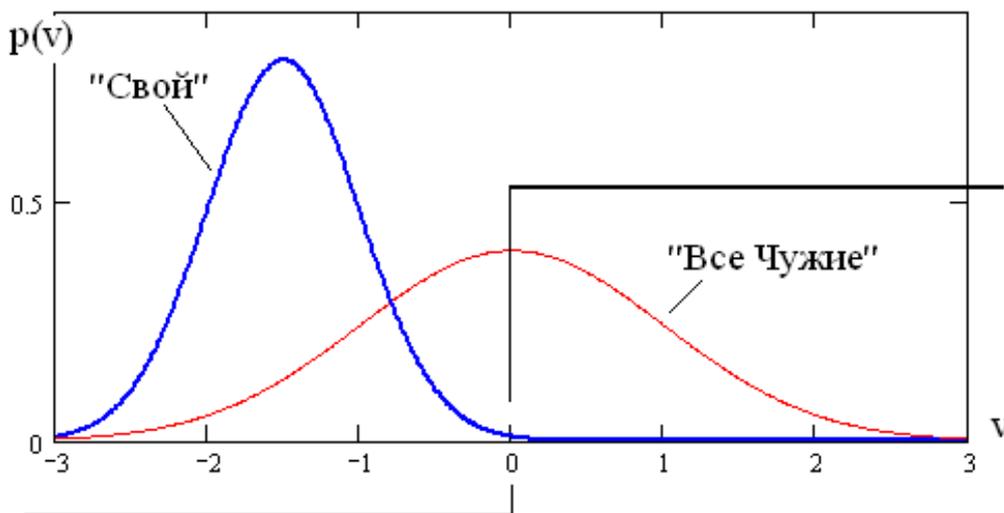


Рис. 3. Пример распределения значений «хорошего» БиоПараметра образа «Свой» и того же БиоПараметра образов «Все Чужие»

Тот факт, что все пороги квантователей расположены в точках математического ожидания образов «Все Чужие», то это дает эффект равновероятного появления состояния «0» и состояния «1» в каждом разряде кода при воздействии на НейроСеть, случайно выбранными образами «Чужой», т.е. энтропия каждого отдельно рассматриваемого разряда кода для случайных образов «Чужой» единична:

$$H_1(\text{«Все Чужие»}) = H("x_i") = -\log_2(0,5) = 1 \text{ бит.} \quad (2)$$

В нашем случае в среде «БиоНейроАвтограф» при обучении нейросети распознаванию примеров образа «Свой» следует задать случайный выходной код [5]. Тогда все весовые коэффициенты нейронов вычисляются следующим образом:

$$\left\{ \begin{array}{l} \mu_i \leftarrow -\frac{E(v_i) - E(\xi_i)}{\sigma(v_i)} \text{ если задан отклик } i\text{-го разряда «0»} \\ \mu_i \leftarrow +\frac{E(v_i) - E(\xi_i)}{\sigma(v_i)} \text{ если задан отклик } i\text{-го разряда «1»} \end{array} \right., \quad (3)$$

где $E(v_i)$ – математическое ожидание i -го БиоПараметра образа «Свой»; $E(\xi_i)$ – математическое ожидание i -го БиоПараметра образов «Все Чужие»; $\sigma(v_i)$ – стандартное отклонение i -го БиоПараметра образа «Свой».

При вычислении весовых коэффициентов по формуле (3), обученная нейросеть откликается на примеры образа «Свой» практически одинаковыми кодами, т.е. энтропия разрядов кода «Свой» оказывается близка к нулевой:

$$H(\text{«Свой»}) = H("v_1, v_2, \dots, v_{256}") \approx 0,01 \text{ бит.} \quad (4)$$

Напротив, энтропия разрядов кодов «Чужой» оказывается много больше, чем энтропия кодов «Свой»:

$$H(\text{«Чужой»}) = H("x_1, x_2, \dots, x_{256}") \approx 56 \gg 0,01 \text{ бит.} \quad (5)$$

Можно говорить о том, что обученная НейроСеть устраняет естественную неопределенность примеров рукописных образов «Свой» и, напротив, усиливает (хэширует) естественную неопределенность примеров рукописных образов «Чужой».

Принципиально важным является то, что обучение НейроСети выполняется очень быстро (от 0,1 до 0,7 с на обычном компьютере). Для оценки скорости обучения следует инициировать клавишу «Обучить сеть» и дождаться смены экранной формы. Кроме того, обучение ведется на малых обучающих выборках объемом от 8 до 20 примеров образа «Свой». Столь малый объем обучающей выборки является достаточным, если позволяет достаточно точно вычислить математическое ожидание и стандартное отклонение по каждому из 416 БиоПараметров образа «Свой».

1.4. Экономия памяти и сокращение времени при тестировании обученной нейросети на малых выборках в пространстве расстояний Хэмминга

В связи с тем, что энтропия каждого разряда кодов «Все Чужие» равна одному биту (2), может возникнуть иллюзия того, что личные криптографические ключи, извлеченные из среды моделирования «БиоНейроАвтограф», имеют высокое качество, т.е. НейроСетевой классификатор имеет огромное число в 2^{256} выходных классов «Чужой». Это далеко не так по причине наличия корреляционной сцепленности разрядов выходного кода. Для нулевой энтропии разрядов (3) должна наблюдаться полная корреляционная сцепленность выходных разрядов кодов «Свой». Для кодов «Чужой-k» должна наблюдаться частичная корреляционная сцепленность разрядов кода «Свой».

Для того чтобы оценить реальное число выходных классов нашей НейроСетевой конструкции, следует воспользоваться рекомендациями ГОСТ Р 52633.3 [10] и перейти от анализа статистик появления обычных кодов к анализу статистик расстояний Хэмминга между кодами:

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

где $"c_i"$ – состояние i -го разряда кода «Свой»; $"x_i"$ – состояние i -го разряда кода «Чужой»; \oplus – операция сложения по модулю два.

Вычисление расстояний Хэмминга (6) имеет простой смысл подсчета числа не совпавших бит у двух сравниваемых кодов. В среде моделирования «БиоНейроАвтограф» не совпавшие биты кода «Свой» и кода «Чужой» отображаются звездочками в режиме «Проверить». На рис. 4 отображена ситуация расхождения кодов в 90 битах.

В случае, если мы используем достаточно большое число случайных рукописных образов «Чужой», мы получим дискретное распределение расстояний Хэмминга с практически нормальным распределением.

Распределение расстояний Хэмминга стремится к нормальному из-за того, что 256-кратное суммирование случайных состояний (10) является сильным нормализатором по «центральной предельной теореме статистики».

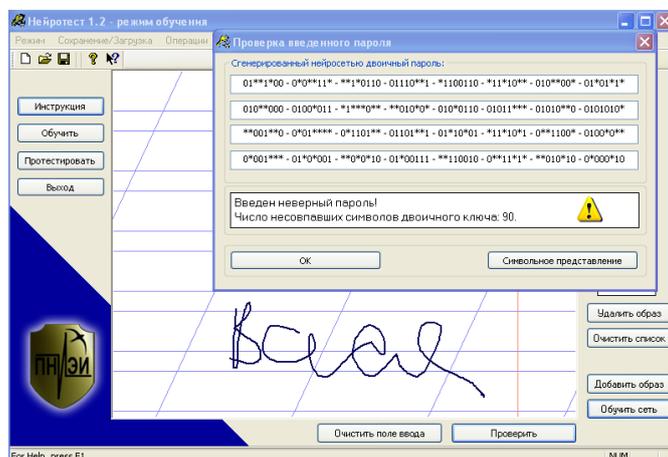


Рис. 4. Режим «Проверить» рукописное слово «Вася» сетью, обученной распознавать слово «Пенза»

Пользуясь гипотезой нормальности, мы можем по математическому ожиданию и стандартному отклонению оценить вероятность, когда код «Чужой» даст полное совпадение с кодом «Свой». В рассматриваемом приложении есть специальный режим «Операции» → «Тестирование на тестовых образах» → «Открыть». В этом случае появляется форма отчета о вычислениях, приведенная на рис. 5.

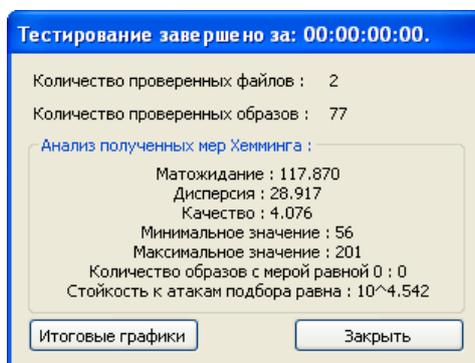


Рис. 5. Экранная форма статистик НейроСетевого классификатора, отображающая результат вычислений по 77 тестовым образам «Чужой», $10^{4.54}$ – попытка атаки случайной подстановки может привести к удаче

Последнее означает, что исследуемая НейроСеть «Пенза» способна различать между собой примерно $10^{4,54} \approx 2^{15}$ классов рукописных образов. Для этого числа классов достаточно коротких кодов, длиной в 15 бит. Реально наблюдаемый 256-битный выходной код НейроСети избыточен. Его 17-кратная избыточность может быть использована для корректировки, случайно возникающих редких ошибок [11] в коде в «Свой».

В первом приближении можно считать, что энтропия выходных кодов НейроСети должна составлять примерно 15 бит вместо 256 «видимых» бит. Еще одним важным моментом является то, что энтропия каждого образа «Чужой» будет разной. Эта ситуация отображена на рис. 6.

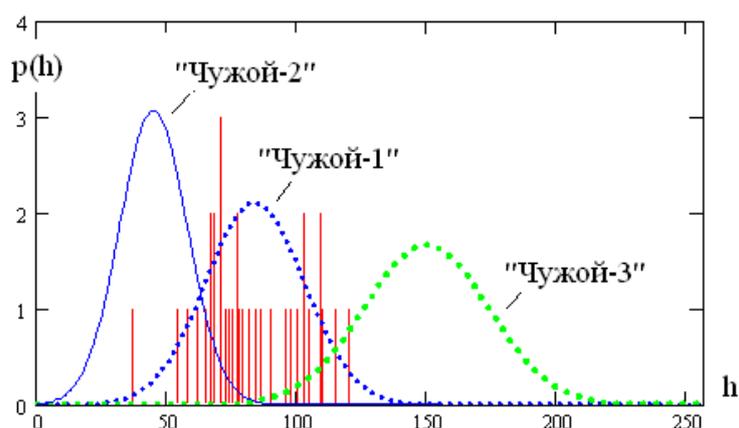


Рис. 6. Эффект взаимной сортировки биометрических образов в пространстве расстояний Хэмминга

Чем дальше математическое ожидание расстояний Хэмминга от точки $h = 0,0$ и чем меньше стандартное отклонение $\sigma(h)$, тем выше энтропия кодов, исследуемого биометрического образа «Чужой». В связи с этим, рассчитав энтропию для группы образов «Чужой», мы легко можем их взаимно упорядочить.

В рамках гипотезы нормального распределения расстояний Хэмминга энтропия образов «Чужой» вычисляется по следующей формуле:

$$\left\{ \begin{array}{l} P_2(h) = \frac{1}{\sigma(h)\sqrt{2\pi}} \int_{-\infty}^1 \exp\left\{ \frac{-(u - E(h))^2}{2(\sigma(h))^2} \right\} du \\ H("x_1, x_2, \dots, x_{256}") \approx -\log_2(P_2(h)) \end{array} \right. . \quad (7)$$

Для нас принципиально важным является то, что вычисление энтропии длинных кодов по Шенону [12] является задачей экспоненциальной вычислительной сложности. Энтропия, оцениваемая в пространстве расстояний Хэмминга (7), является задачей с линейной вычислительной сложностью. При переходе от обычного наблюдения длинных кодов в пространство расстояний Хэмминга наблюдается гигантское ускорение вычислений энтропии.

Если бы мы решили оставаться в рамках классической статистики, то для корректного вычисления вероятности ошибок второго рода – P_2 (ошибочного признания образа «Чужой» как образ «Свой») – нам пришлось бы использовать примерно 100 000 примеров образов «Чужой». Если же мы перейдем в пространство расстояний Хэмминга (6), то для вычисления математического ожидания – $E(h)$ и стандартного отклонения $\sigma(h)$ достаточно 20, случайно выбранных примеров образов «Чужой». Мы наблюдаем эффект сокращения требуемого объема памяти примерно в 5000 раз и во столько же раз ускорение вычислений.

1.5. Экономия памяти и сокращение времени при тестировании обученной НейроСети на малых выборках в пространстве корреляционной сцепленности разрядов длинных кодов

В среде моделирования «БиоНейроАвтограф» предусмотрен файл «testKeys.txt», где записываются двоичные ключи, полученные на 256 выходах нейросети при ее тестировании. На рис. 7 приведены два

ключа-отклика нейросети «Пенза», полученные при предъявлении двух примеров одного образа «Хопер».

Двоичный ключ:

```
010110000111101001100111110100110101101001101011001000100101110001110111101011100
11100100001010011101001110000100101001101000110101100101100100111111100000001001
010010010101100100101001110010010110010101001001100110010000110110100101000111010
0110101001010
```

Двоичный ключ:

```
10011000111101100100010111010101110100101110100100101000110011101010111100111110
010111100010011110010001101001011111110110001010110010110101111010111000001001
0000100010011010001011011110100101100001111110100010001000011110110110100001001
1110111000101
```

Рис. 7. Два ключа, длиной 256 бит, полученные как отклики нейросети на два примера одного образа «Хопер»

Из рис. 7 видно, что первая и вторая битовые последовательности содержат много общего, но они же имеют и существенные расхождения. Это означает, что корреляция этих выходных последовательностей может быть оценена прямым вычислением коэффициентов корреляции между ними, т.е., если обозначить бинарные последовательности файла «testKeys.txt» как $\{x_1, x_2, \dots, x_{21}\}$, то мы можем вычислить нужные нам коэффициенты корреляции и корреляционную матрицу в целом:

$$\begin{bmatrix} 1 & r(x_1, x_2) & \dots & r(x_1, x_{21}) \\ r(x_1, x_2) & 1 & r(x_2, x_3) & \dots \\ \dots & \dots & \dots & \dots \\ r(x_1, x_{21}) & r(x_2, x_{21}) & \dots & 1 \end{bmatrix}, \quad (8)$$

где

$$r("x_k", "x_j") = \frac{1}{256} \sum_{i=1}^{256} \frac{(E("x_{k_i}") - "x_{k_i}")(E("x_{j_i}") - "x_{j_i}"))}{\sigma("x_{k_i}") \cdot \sigma("x_{j_i}"))}. \quad (9)$$

Для того чтобы далее вычислить коэффициент эквивалентной симметричной матрицы $\tilde{\gamma}$, следует усреднить модули всех коэффициен-

тов корреляции матрицы (8), находящихся вне ее диагонали [13] и оценить их стандартное отклонение.

Если мы имеем дело с 20 примерами образа «Хонер» и образа «Сура», то сможем получить матрицы коэффициентов корреляции 20×20 , которые будут иметь 180 разных коэффициентов корреляции. На рис. 8 даны распределения значений коэффициентов корреляции, рассматриваемых образов, построенные в рамках гипотезы нормальности их распределений.

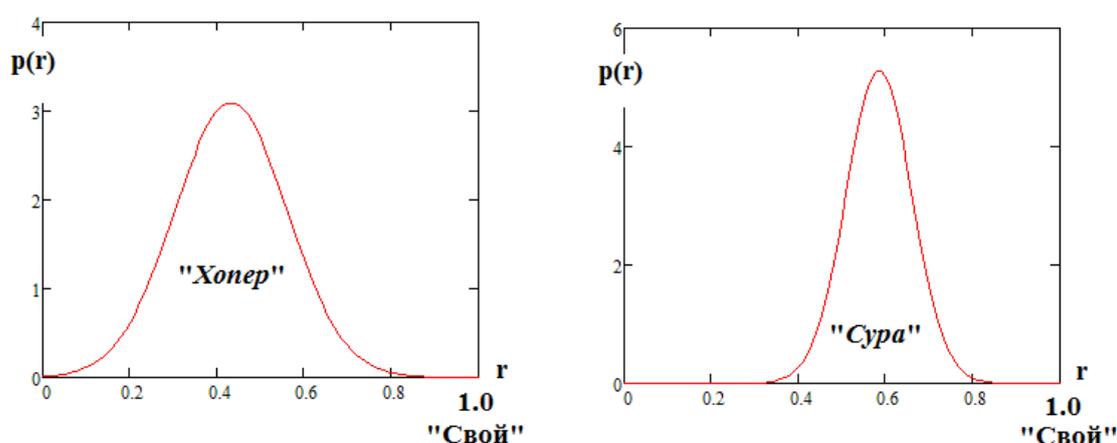


Рис. 8. Распределение расстояний корреляционной сцепленности между ключами от примеров образа «Хонер» и ключами от образа «Сура» (предельное значение корреляции «Свой» в правой части рисунка $r = 1,0$)

Как итог, мы можем в дополнение к энтропии Хэмминга (7) построить аналогичную по содержанию энтропию корреляционной сцепленности разрядов длинного кода

$$\left\{ \begin{array}{l} P_2(r) = \frac{1}{\sigma(r)\sqrt{2\pi}} \int_{0.99}^{\infty} \exp\left\{ \frac{-(u - E(r))^2}{2(\sigma(r))^2} \right\} du \\ H("x_1, x_2, \dots, x_{256}") \approx -\log_2(P_2(r)) \end{array} \right. . \quad (10)$$

Отметим, что и в случае вычисления энтропии корреляционной сцепленности по сравнению с вычислением энтропии Шеннона мы получаем выигрыш по сокращению памяти примерно 5 000 раз, а выигрыш

по ускорению вычисления оказывается примерно 300 раз. Это примерно такой же показатель, что и для вычислений энтропии в пространстве расстояний Хэмминга, однако выражения (8) и (9) существенно отличаются от выражения (6) по вычислительным затратам. Главное же состоит в том, что для вычисления энтропии корреляционной сцепленности (10) не нужна информация о значении разрядов кода «Свой». Это открывает возможность вычисления энтропии неизвестно чему обученной НейроСети.

ГЛАВА ВТОРАЯ

ГИПЕРУСКОРЕНИЕ ПЕРЕБОРА ОБРАЗОВ «ЧУЖОЙ» ПРИ ИЗВЛЕЧЕНИИ ЗНАНИЙ ИЗ ТАБЛИЦ ОБУЧЕННОЙ СЕТИ ПЕРСЕПТРОНОВ

2.1. Извлечение знаний из НейроСетевого преобразователя биометрия-код путем направленного синтеза образов «Чужой» с монотонно уменьшающейся энтропией

В связи с введением в действие в России базового стандарта ГОСТ Р 52633.0–2006 [14] возникла необходимость численного решения обратной задачи нейросетевой биометрии [15–17]. Эта задача была решена в рамках НИР «Биометрия» в 2009 г. (Исполнитель – АО «ПНИЭИ» г. Пенза, Заказчик – «ГНИИИ ПТЗИ ФСТЭК России» г. Воронеж).

В среде моделирования «БиоНейроАвтограф» есть функция сохранения обучающей базы биометрических примеров в файл «MyImages.dat». Для рукописного образа «Пенза» один пример будет занимать объем 1,2 Кб. Если считать этот образ типовым, то 100 000 образов «Чужой» по 20 примеров каждый будут занимать примерно 2 Гб долговременной памяти. Для современного компьютера это вполне приемлемый объем требуемой памяти, соответственно тестирование на таком объеме базы данных «Чужой» вполне возможно.

Проблема состоит в ином: в нужный момент базы такого объема, созданной по требованиям ГОСТ Р 52633.1–2009 [18], может не оказаться под рукой. В этом случае можно воспользоваться меньшей базой в 10 000 биометрических образов «Чужой». Распределение энтропии для образов базы такого объема отображено на рис. 9.

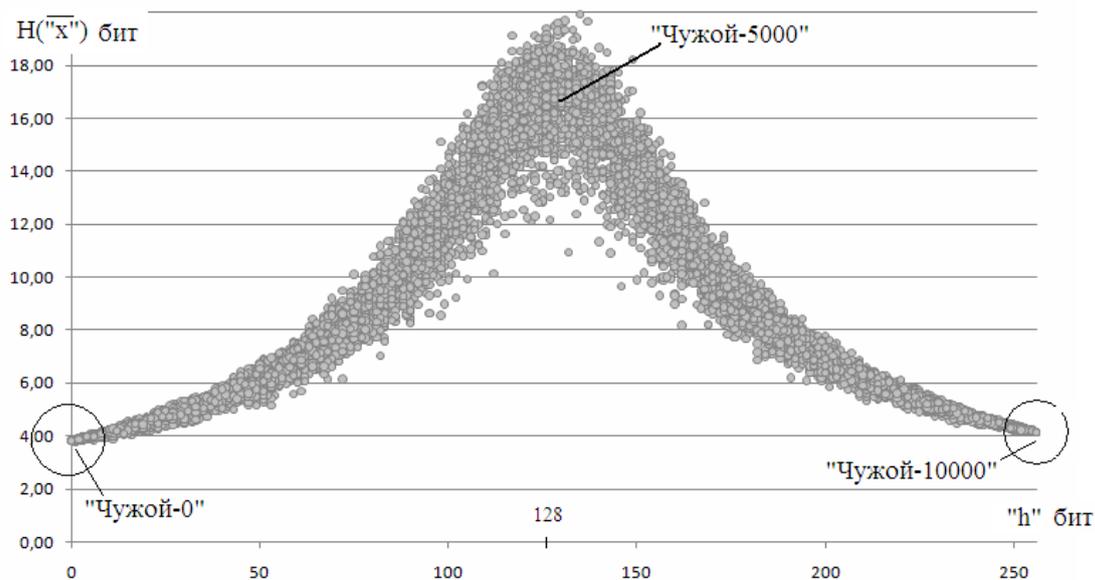


Рис. 9. Два минимума распределения значений энтропии образов «Чужой», разнесенные с учетом расстояний Хэмминга между центрами их кодовых откликов

Из рис. 9 видно, что распределение значений энтропий имеет вид «палатки» и обладает двумя минимумами. Такой вид распределения обусловлен наличием симметрии образов «Свой» и его инверсии для сети персептронов, автоматически обученных по ГОСТ Р 52633.5. Появление этой симметрии поясняет рис. 10.

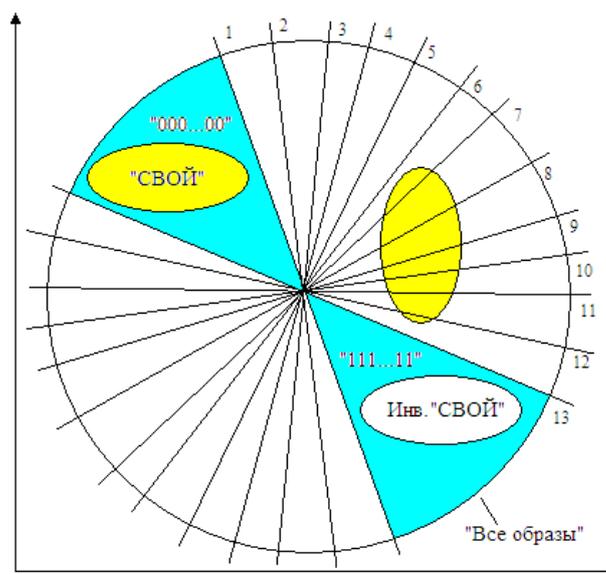


Рис. 10. Симметрия образа «Свой» и его инверсии, наблюдаемая у однослойных сетей искусственных нейронов с линейным накоплением

Алгоритм автоматического обучения ГОСТ Р 52633.5 построен на том, что все разделяющие гиперплоскости искусственных нейронов проходят через центр 416-мерной области «Все Чужие». Если мы возьмем любое двухмерное сечение 416-мерной гиперсферы, то разделяющие гиперплоскости становятся линиями, проходящими через центр окружности «Все Чужие». На окружности всегда образуются два больших сектора, попадают эллипсы распределения данных «Свой» и его инверсных данных. Такая картина будет повторяться в любом двухмерном сечении. Ни одна разделяющая гиперплоскость 256 персептронов не может пересекать эллипс данных «Свой» и эллипс инверсных ему данных по отношению к центру данных «Все Чужие». Именно из-за такой симметрии коды, порождаемые примерами образа «Свой» и его инверсии, оказываются очень стабильными. Напротив, каждый образ «Чужой» многократно пересекается гиперплоскостями части из искусственных нейронов. Как следствие возникает эффект нестабильность разрядов выходных кодов «Чужой» при незначительных изменениях входных биометрических параметров.

Очевидно, что правые и левые коды «Чужой» с самой низкой энтропией будут давать коды, наиболее близкие к коду «Свой» или к его инверсному коду. Для организации атаки по извлечению знаний из НейроСети нужно выделить две группы образов «Чужой» с минимальной энтропией объемом примерно по 50 образов, как это показано на рис. 9. В итоге мы получили вместо 10 000 исходных образов «Чужой» всего 100 образов.

Далее следует восстановить исходную численность выделенных образов путем их скрещивания между собой алгоритмом ГОСТ Р 52633.2 [19]. На рис. 11 иллюстрируется процедура скрещивания между собой двух образов-родителей и получение от них одного, двух, трех образов потомков.

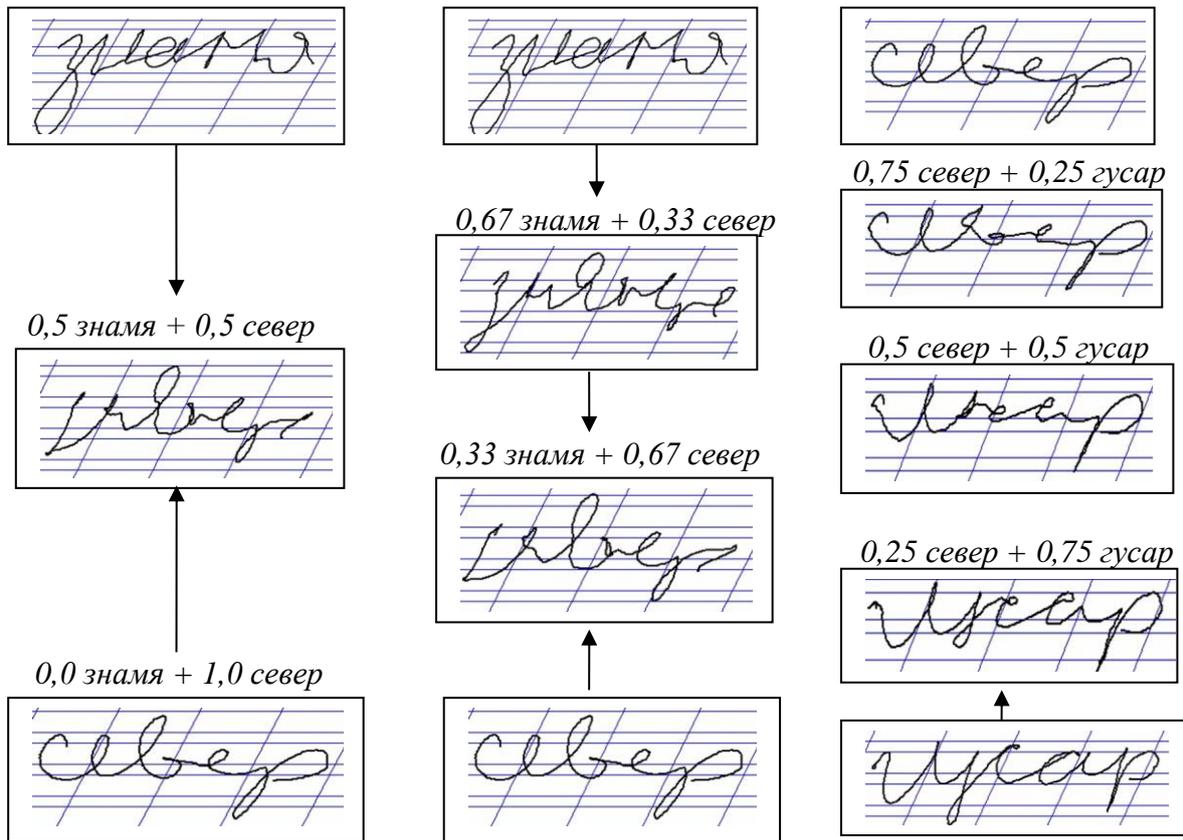


Рис. 11. Примеры синтеза одного, двух и трех образов-потомков скрещиванием двух образов-родителей

После восстановления численности тестовых образов «Чужой» во втором поколении следует повторить атаку направленного подбора. Если повторять атаку направленного подбора порядка 50 поколений, то в итоге удастся извлечь из нейросети порядка 97 % знаний о размещенном в ней коде ключа «Свой» и о биометрических параметрах образа «Свой».

Получается, что по исходной выборке в 10 000 естественных биометрических образов «Чужой» удастся решать обратную задачу нейросетевой биометрии с приемлемой для практики достоверностью определяемых параметров.

2.2. Оценка достижимого гиперускорения выполнения направленного перебора при переходе от анализа данных в НейроСтатике к анализу данных в НейроДинамике

Описанное в предыдущем разделе решение обратной задачи биометрии выполняется примерно за 20 мин на обычной вычислительной машине. Это стало технически возможно из-за того, что база из 10 000 тестовых образов «Чужой», объемом в 2 Гб, способна разместиться в памяти компьютера. Однако, если бы мы пошли по пути изначального синтеза полной базы образов «Чужой» для реализации во всех 50 поколениях и размещения данных в памяти компьютера, то нам потребовалось бы 2^{50} Гб. Такой памяти нет у современных компьютеров. В связи с этим, схема экономии памяти, когда отсортированные данные уничтожаются, оказалась крайне экономичной. Обобщенная схема проведения численного эксперимента по решению обратной задачи НейроСетевой биометрии с экономией памяти приведена на рис. 12.



Рис. 12. Снижение требований к памяти компьютера при хранении и использовании данных только одного «текущего» поколения в 10 000 образов «Чужой»

Следует также отметить, что при выполнении операций обращения матриц НейроСетевых функционалов модуляция биометрических данных выполняется не только морфинг-скрещиванием образов-родителей, но и добавлением к исходным данным мутаций. На рис. 13 отображена схема аддитивного подмешивания мутаций к скрещиваемым данным.

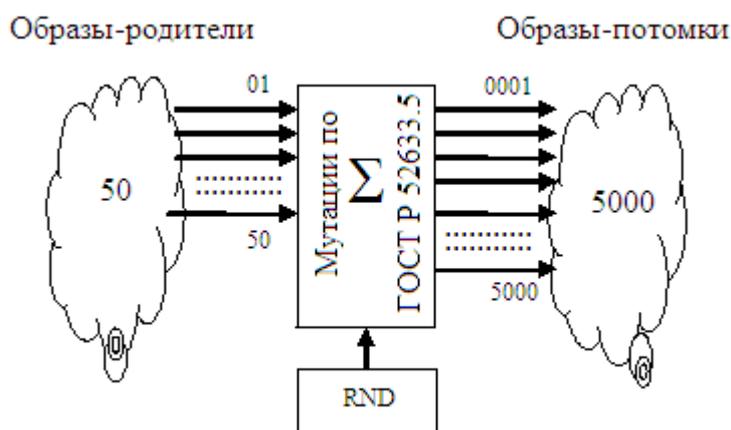


Рис. 13. Добавление малого случайного шума мутаций к образам «Чужой» по ГОСТ Р 52633.2–2010

Кроме огромной экономии памяти, порядка 2^{49} Гб, вычислительная схема рис. 12 и 13 дополнительно дает огромное ускорение НейроСетевых вычислений, возникающее из-за сокращения ненужных операций или их условного распараллеливания.

Когда речь идет о нейронных сетях, то очевидным является линейное распараллеливание нейровычислений. Современные процессоры могут иметь от 4 до 4096 ядер [20], т.е., располагая многоядерным процессором, теоретически мы можем ускорить вычисления в интервале от 4 до 4096 раз.

Те процедуры, которые рассмотрены выше, позволяют выполнять гиперускорение НейроСетевых направленных переборов даже на одном ядре в пространстве расстояний Хэмминга. Мы фактически на одном ядре имеем в каждом поколении 50-кратное ускорение (отбрасывается

98 % образов, сохраняется только 2 % образов с минимальной энтропией). Так как эта процедура повторяется в каждом из 50 поколений, параллельно с экономией памяти возникает ускорение вычислений в 50^{50} раз. Столь значительные ускорения трудно воспринимать и сопоставлять. Одним из способов, облегчающих восприятие, является перевод показателей ускорения в «гугл» систему счисления. Один «гугл» составляет 10^{100} , соответственно величина 10^{85} должна составить 0,85 часть «гугл», величина 10^{200} должна интерпретироваться как величина, соответствующая 2,0 «гугл» единицам. Исходя из этих представлений, построена таблица оценки достижимых на обычной вычислительной машине ускорений за счет неявного гиперраспараллеливания вычислений на одном ядре процессора (табл. 1).

Таблица 1

Оценка достижимых ускорений

Число поколений	40	42	44	46	48	50	52	54	56	58	60
«Гугл» показатель	0,680	0,714	0,748	0,782	0,812	0,85	0,884	0,918	0,951	0,985	1,02

Из табл. 1 следует, что уже при 60 поколениях рассмотренные процедуры гиперраспараллеливания вычислений позволяют получить ускорение в один «гугл» раз на обычном компьютере. Именно из-за столь значительного ускорения и удается решать обратные задачи нейросетевой биометрии.

Столь значительное ускорение вычислений обусловлено переходом от использования нейронных сетей в статике к поддержке их постоянных динамических переходов из одного состояния в другое. При обработке первого поколения образов «Чужой» постоянное и изменение состояний НейроСети обеспечивается подключением ко входам НейроСети 20 примеров одного образа «Чужой». Именно благодаря изменениям выходных состояний НейроСети появляется техническая воз-

возможность вычислить амплитуды вероятности появления дискретных расстояний Хэмминга или вероятность появления различных непрерывных состояний корреляционной сцепленности.

2.3. БИОНИКА – копирование естественных НейроСетевых структур людей и других живых сущест, непрерывно находящихся в динамике и имеющих внутренние механизмы многоуровневого квантования

Следует отметить, что естественные нейроны людей и животных организованы очень сложно. Модели искусственных нейронов (см. рис. 1) весьма и весьма примитивны и отражают суть естественных процессов только в первом приближении. На самом деле естественные нейроны одновременно являются и вычислителями, и модемами, передающими данные на очень большие расстояния (до одного метра при линейных размерах тела самого нейрона порядка 0,0001 м) [21]. Как утверждает Уосерменн [22], у человека имеется примерно 10^{11} естественных биологических нейронов, которые связаны между собой в некоторый клубок 10^{15} связями. Число входов у нейрона и число выходов у его длинного аксона может быть разным, однако у людей существуют гигантские пирамидальные нейроны, имеющие до 10 000 входов [3], т.е. некоторые из нас на подсознательном уровне способны решать 10 000-мерные задачи.

Важным отличием модели нейронов, показанных на рис. 1, от естественных нейронов является то, что они предполагают только бинарные отклики искусственных нейронов. Реальные нейроны гораздо более сложные [5, 23]. Они способны давать решения, закодированные несколькими импульсами, т.е. они имеют многоуровневые выходные квантователи [24]. Формально это может быть учтено простым изменением формы выходных нелинейных элементов искусственных нейронов, как это показано на рис. 13.

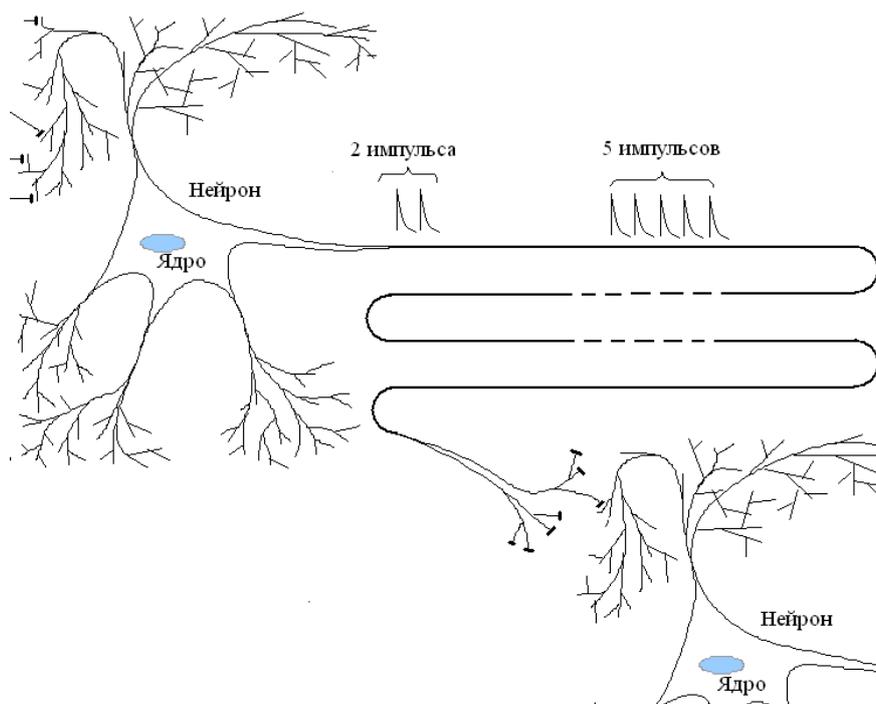


Рис. 13. Естественный нейрон, одновременно выполняющий функцию вычислителя и функцию модема, передающего данные по длинной линии (аксону), которая примерно в 10 000 раз длиннее тела самого нейрона

Как работают многоуровневые выходные квантователи у естественных биологических нейронов доподлинно неизвестно. Вполне возможно, что каждый ион, проскочивший переход с выходного аксона предыдущего нейрона на входной дендрит следующего нейрона, дает свой импульс. Если переходит несколько ионов одного типа, то возникает пачка из нескольких импульсов тока в аксоне. Если происходит туннельный переход нескольких разных ионов с одного нейрона на другой, то должны возникать импульсы тока разной амплитуды. Для каждого типа ионов должна возникать своя амплитуда токового импульса в аксоне.

Для нас с вами нет смысла пытаться уточнять причины, порождающие квантовые эффекты на уровне ионообмена естественных биологических нейронов. Будут порождать эти эффекты тонкие ионные туннельные барьеры [21, 23] между аксонами и дендритами или нанотрубки [25] – для нас не имеет никакого значения. Важен только сам факт наличия кван-

тователей на выходах искусственных нейронов на выходе их элементов, отвечающих за накопление (обогащение) входных данных (рис. 14).

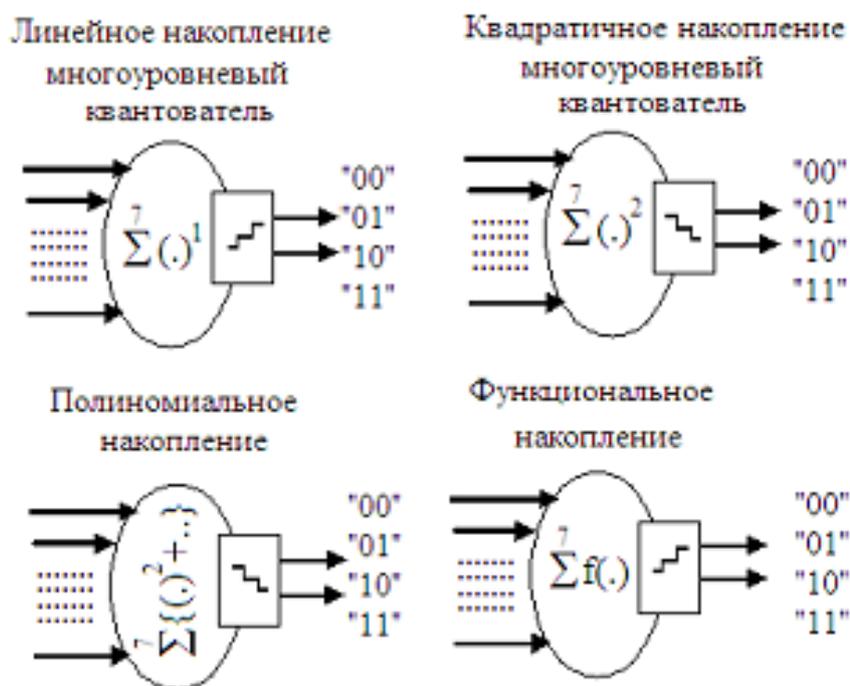


Рис. 14. Формальные модели искусственных нейронов с многоуровневыми выходными НейроКвантователями

Принципиальным также является то, что естественные биологические нейроны людей и животных находятся в постоянном самовозбуждении (в режиме поддержки НейроДинамики). Насколько такой режим может ускорить вычисления перебором состояний некоторого нейросетевого вычислителя показано в предыдущем разделе.

Главное для темы данной работы состоит в том, что в моделях нейрона, в искусственных нейронах существуют квантователи (бинарные или многоуровневые). Именно благодаря этому могут возникнуть эффекты НейроДинамики, приводящие к примерно таким же результатам, как приводят эффекты квантовой суперпозиции микробиологических объектов: молекул, атомов, ионов (котов Шредингера).

Вопрос только в том, как овладеть положительными эффектами НейроДинамики и применять их, например, для ускорения переборов на

обычных компьютерах в миллиарды раз. Видимо, в наших головах изначально был создан НейроДинамический квантовый вычислитель, постоянно находящийся в шумах, поддерживающих в нем эффекты квантовой суперпозиции. При этом наблюдаемые нами шумы электроэнцефалограмм есть не что иное как побочное электромагнитное излучение квантового НейроДинамического компьютера в нашей голове.

Косвенно об этом можно судить по работам С. М. Гончарова и А. Е. Боршевникова. Суть их работ состояла из контроля шумов электроэнцефалограммы в момент, когда человеку предъявлялись цифры 0, 1, ..., 9 [26–28]. При этом нейросеть заранее обучалась распознавать электроэнцефалограммы, порождаемые наблюдаемыми человеком цифрами, т.е. даже простейшие сети с накоплением данных в линейном пространстве, обученные по ГОСТ Р 52633.5, легко справляются с задачей распознавания шума электроэнцефалограмм. Для них это вовсе не шум, а вполне понятный поток шумоподобных НейроДанных (рис. 15).

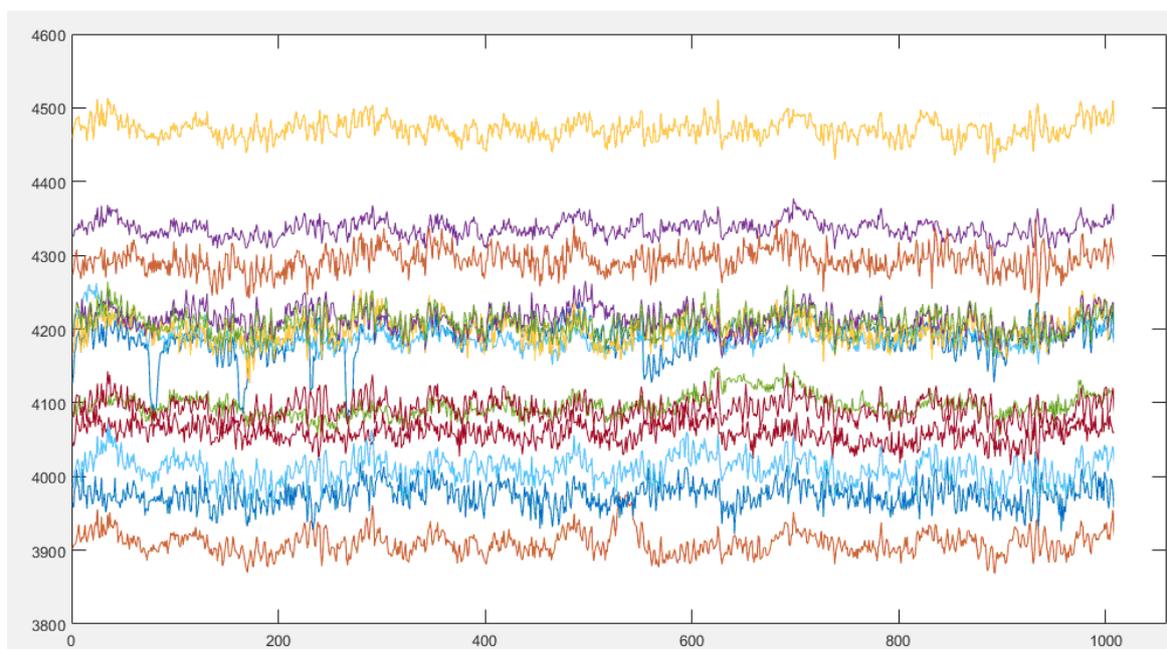


Рис. 15. Примеры электроэнцефалограмм, снятых с 14 электродов на голове испытуемого человека при наблюдении им одной из десяти цифр (0, 1, ..., 9); данные из работы Гончарова и Боршевникова [26]

2.4. Квантовые процессоры как перспектива совершенствования машин фон Неймана в период с 1980 по 2011 г.

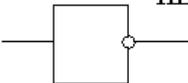
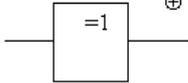
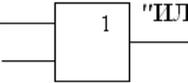
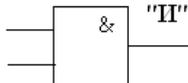
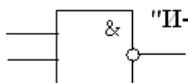
Следует отметить, что НейроСетевые процессоры и машины архитектуры фон Неймана [27] начали развиваться примерно в одно и то же время. За прошедшие 80 лет развития логико-цифровые машины заполнили весь мир, а НейроСетевые процессоры развивались гораздо медленнее. Ситуация начала меняться только в 20-х гг. XXI в.

Проблемы машин с архитектурой фон Неймана были очевидны достаточно давно. Давно было понятно, что их нужно ускорять, нужны новые идеи в этом направлении. Первым идею новых квантовых принципов работы вычислителей высказал в 1980 г. М. Ю. Манин [30, 31]. Идея, видимо, витала в воздухе, так как практически то же самое высказали Ричард Фенбаум в 1981 г., Пол Бениофф в 1982 г., Стивен Визнер в 1983 г.

Общая идея квантовых компьютеров в первом приближении может быть сведена к замене обычной логики обычных компьютеров [32, 33] на квантовую логику квантовых компьютеров. Эту ситуацию иллюстрирует табл. 2 обычных и квантовых логических элементов.

Очевидно, что матрицы или их фрагменты (гейты) можно запрограммировать под обычный компьютер, получив тем самым удобные языки для программных симуляторов квантово-матричных вычислений [34]. К сожалению, этот путь является бесперспективным, так как не приводит к ускорению вычислений. Этот путь не более чем экономит время программистов, но этот фактор не является существенным. Промышленного применения таких языков программирования, как «Quipper» или «Haskell», скорее всего, не будет.

Таблица 2

Обычная Булева логика или элементы логических цепей	Гейты квантовой логики или элементы квантовых логической цепей
 <p>"НЕТ"</p>	$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ <p>Вентиль Адамара</p>
 <p>\oplus</p>	$\begin{bmatrix} 1 & 0 \\ 0 & e^{j\frac{\pi}{4}} \end{bmatrix}$ <p>Фазовый вентиль</p>
 <p>"ИЛИ"</p>	$\begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}$ <p>Вентиль Паули</p>
 <p>"И"</p>	$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ <p>Двухкубитный инвертор</p>
 <p>"И-НЕТ"</p>	
.....

Происходит это по той причине, что квантовые машины, программно воспроизводящие 10 КуБит, никому не нужны. В частности для практического применения алгоритма Питера Шора [34] нужно сегодня создавать аппаратно квантовый Фурье-процессор на 2048 КуБит. Никакая из современных вычислительных машин с архитектурой фон Неймана программного эмулятора квантового Фурье-процессора такой размерности не потянет. Специалистам по применению физической реализации гейтов и тензоров придется ждать неопределенное время, пока Силиконовая долина, Китай или Сколково не обеспечат их серийно производимыми микросхемами аппаратно-полноценных гейтов квантовой логики или тензоров. Только в этом случае мы все получим предсказанные в теории квантовых вычислений гиперускорения.

Существует даже теорема о том, что моделирование уравнений Шредингера (квантовых вычислений с использованием котов Шредингера) на обычных компьютерах бесполезно. Это совершенно правильная

теорема – решение дифференциальных уравнений Шредингера (моделирование уравнений Шредингера) для процессоров с архитектурой фон Неймана или для машин Тьюринга является задачей экспоненциальной вычислительной сложности. Совершенно иная ситуация возникает, если мы получаем (поддерживаем) эффекты квантовой суперпозиции для уравнений НейроДинамики. Моделирование сетей искусственных нейронных на обычных вычислительных машинах – это задача линейной вычислительной сложности. Это означает, что моделировать стаю «котов Шредингера» на обычной машине действительно не имеет смысла: начиная с некоторого числа «котов Шредингера» машина обязательно повиснет. Если же мы будем моделировать нейронные сети (стаю «собак Павлова»), то нам оказываются доступны НейроДинамические задачи очень высокой входной и выходной размерности.

Получается, что, оставаясь в парадигме архитектуры процессоров фон Неймана (память можно обменять на быстродействие), с 1980 г. до 2011 г. физико-математическая общественность была уверена в том, что единственным способом значительно увеличить быстродействие вычислений является миниатюризация вычислительных элементов (переход к использованию стаи «котов Шредингера» с наноразмерами). Ситуация кардинально изменилась в 2011 г. с принятием в России ГОСТ Р 52633.3 [10]. Если действовать в духе этого документа возможно быстрое тестирование нейронных сетей при одновременном сокращении объема памяти и гиперувеличении скорости вычислений на машине с архитектурой фон Неймана. Далее нужно сделать последний шаг. Вместо того, чтобы тестировать нейросети, нужно научиться писать на них ускорители, работающие в НейроДинамике и ускоряющие переборы известных математических задач. При этом жидкий гелий и новая элементная база для квантовых вычислений НейроДинамики не нужны. Вполне достаточно уже имеющихся вычислительных машин

с архитектурой фон Неймана, которые будут поддерживать НейроДинамику клубка некоторым образом сцепленных искусственных нейросетей, подобно тому, как это реализовано в наших с вами естественных мозгах. При этом, скорее всего, программирование нижнего уровня таких НейроСетевых процессоров, будет связано с формированием их архитектуры (сколько нейронов, сколько входов у нейронов, сколько слоев у НейроСети, каким механизмом должна поддерживаться модуляция данных на входах НейроСети, как должны пережевываться спектральные линии Хэминга нейронами следующего уровня). Программирование того, что называют сегодня «сильным» искусственным интеллектом, скорее всего, будет связано с поддержкой НейроДинамики на разных уровнях обработки.

2.5. Неопределенность Гейзенберга для НейроДинамики (либо ускорение вычислений, либо повышение их достоверности)

Следует отметить, что один из важнейших постулатов квантовой механики – это принцип неопределенности Гейзенберга [35], в соответствии с ним для микрочастицы в конкретный момент времени нельзя однозначно указать и ее координаты и ее импульс (скорость). И то, и другое определяется только в паре (их произведение совпадает с половиной постоянной Планка).

Видимо, такая же ситуация характерна не только для динамического (дифференциального) уравнения Шредингера. Видимо, такая же ситуация характерна и для НейроДинамических уравнений, тем или иным образом сцепленных искусственных нейронов.

Выше по тексту мы пытались объяснить причины гиперускорений НейроВычислений, возникающих при многократном переходе от модифицированных континуальных данных к их спектральным линиям Хэм-

минга. 20 переходов из 416-мерных континуальных пространств в 256-мерное дискретное пространство по ГОСТ Р 52633.3 дает примерно 5000 выигрыш по памяти и примерно выигрыш в 250 раз по быстродействию на одном ядре процессора с архитектурой фон Неймана. Шестьдесят таких переходов дает экономию памяти порядка 2^{49} Гб и ускорение вычислений направленным перебором примерно в 10^{100} раз (в один «гугл» раз). Все это может повторить и проверить любой из читателей самостоятельно.

Далее следует обратить особое внимание на то, что НейроДинамика и квантовая механика вполне могут быть использованы не только для ускорения вычислений, но и для повышения их достоверности. В следующей главе мы попытаемся показать, как это реализуется на практике. В этой главе мы обращаем внимание читателя на то, что в квантовой механике «котов Шредингера» вопрос о методах многократного повышения точности и достоверности вычислений или гиперуточнения статистических оценок вообще не рассматривается. Этот теоретически важный вопрос является обратной стороной неопределенности Гейзенберга, а самое главное, что он давно уже решен на практике.

Уже в середине прошлого века у криминалистов появилась практика высокоточного спектрального анализа микропроб примесей. Предположим, что криминалисты обнаруживают у подозреваемого очень точные весы. Следствию нужно ответить на вопрос: зачем подозреваемому такой дорогой и такой точный инструмент в его лачуге? Что подозреваемый взвешивал на этих весах?

Для того чтобы ответить на этот вопрос, криминалист берет вату, смачивает ее в спирте, протирает ею чашу весов, далее вату помещают в пробирку. При анализе вату сжигают, а свет пламени фокусируют и направляют на призму, как это показано в левой части рис. 16.

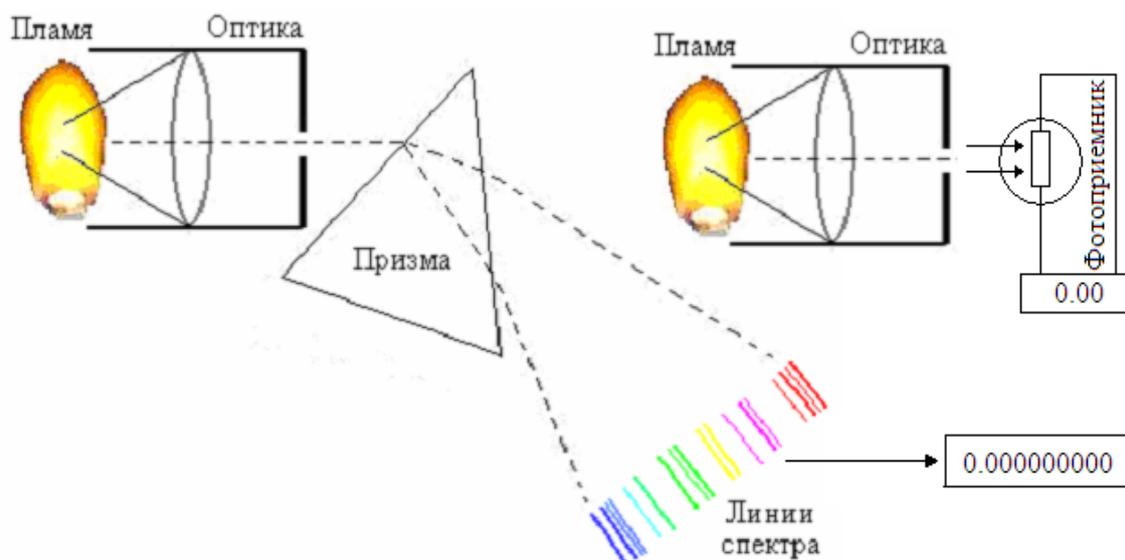


Рис. 16. Схема анализа спектральных линий пламени для обнаружения в сжигаемой пробе нано- и пиковключений стороннего вещества (например, золотой пыли)

Если бы через призму проходил солнечный свет, то после призмы мы бы увидели сплошную радуку без полосок. В нашем случае спектр оказывается полосатым, отображаются полоски, соответствующие возбужденным молекулам кислорода, спирта и горячей ваты. Если теперь накрыть все полоски цветного спектра линиями непрозрачной маски, то свет должен полностью исчезнуть. Это было бы так, если бы на горячей вате не было примесей. Между яркими линиями горения «чистой» ваты проявятся менее яркие линии нанопримесей. Спектральные линии нанопримесей фотографируют с большой экспозицией, а потом эксперт исследует фотографию. Факт обнаружения спектральных линий золота, взрывчатки или наркотиков отражается в заключении спектральной криминалистической экспертизы.

Обычные континуальные методы химического анализа (взвешивание, титрование, просвечивание, и т.д.) способны обнаружить в пробе порядка 0,1 % объема примеси от объема основного вещества (см. правую часть рис. 16). Переход к анализу спектральных линий позволяет увеличить чувствительность или точность метода примерно в миллион

раз. Континуальные методы спектрального анализа естественных молекул позволяют получить только три значащих цифры объемных соотношений примесей. Переход к анализу линий спектра молекул открывает совершенно иные технические возможности.

Тот факт, что спектральные измерения оказываются высокоточными, целиком обусловлен дискретным характером задачи. «Коты Шредингера» в этом случае не мешают ее решению, они сгорают в пламени ваты, смоченной спиртом. При этом «коты Шредингера» золотой пыли дают только спектральные линии золота. «Коты Шредингера» ваты, спирта и кислорода дают только свои спектральные линии (ваты, спирта и кислорода). Если эти спектральные линии горения основного вещества закрыть маской, то они не будут мешать видеть слабые спектральные линии золота между ними. Кроме того, слабые спектральные линии золота всегда можно усилить, увеличив экспозицию засветки фотодокумента. Длина волны спектральной линии золота, отыскиваемой экспертом криминалистом на фотографии, должна составлять 330,83 нм в соответствии с отечественным стандартом ГОСТ Р 27973.1 [36].

Если мы будем пользоваться скобками Дирака [37] аппарата квантовой механики, то записывать эту спектральную линию мы должны следующим образом: $\Psi|330,83\rangle$. Для понимания содержания данной работы не требуется изучение глубин линейной алгебры и привыкания к чтению скобок Дирака. Эта книга ориентирована на людей, обладающих опытом программирования на каком-либо языке. Формальная запись спектральной линии золота в рамках данной работы должна быть следующей: $\Psi(\langle 330,83 \rangle)$ или $\Psi(\langle \text{золото} \rangle)$. Символ « $\Psi(\cdot)$ » наследуется от квантовой механики и означает амплитуду вероятности появления, соответствующей спектральной линии с дискретным положением – «330,83» нанометра или «золото». При программировании приходится различать континуальные (непрерывные) и дискретные переменные. В нашем слу-

чае амплитуда вероятности спектральной линии $\Psi(\cdot)$ является непрерывной величиной, а длина волны в нанометрах является дискретной величиной и потому выделена кавычками. При программировании текстовые или дискретные переменные всегда выделяются кавычками (например, имя читаемого файла записывается как «золото.txt»).

ГЛАВА ТРЕТЬЯ

НЕЙРОСЕТЕВОЕ ОБОБЩЕНИЕ НЕСКОЛЬКИХ СТАТИСТИЧЕСКИХ КРИТЕРИЕВ ПРОВЕРКИ ГИПОТЕЗЫ НОРМАЛЬНОГО РАСПРЕДЕЛЕНИЯ МАЛЫХ ВЫБОРОК В НЕЙРОСТАТИКЕ

3.1. Нейросетевое обобщение классического критерия хи-квадрат (1900 г.) и критерия Крамера – фон Мизеса (1928 г.)

Современная математическая статистика в том виде, какой мы ее знаем, опирается на хи-квадрат критерий Пирсона, построенный им в 1900 г. Эта математическая конструкция оказалась популярной из-за того, что она проста и долгое время альтернативы ей не было. К сожалению, на малых выборках хи-квадрат критерий плохо работает. Эта ситуация иллюстрируется распределением значений состояний хи-квадрат критерия (рис. 17), возникающих при решении задачи линейного разделения малых выборок в 16 опытов для данных с нормальным и равномерным распределением значений.

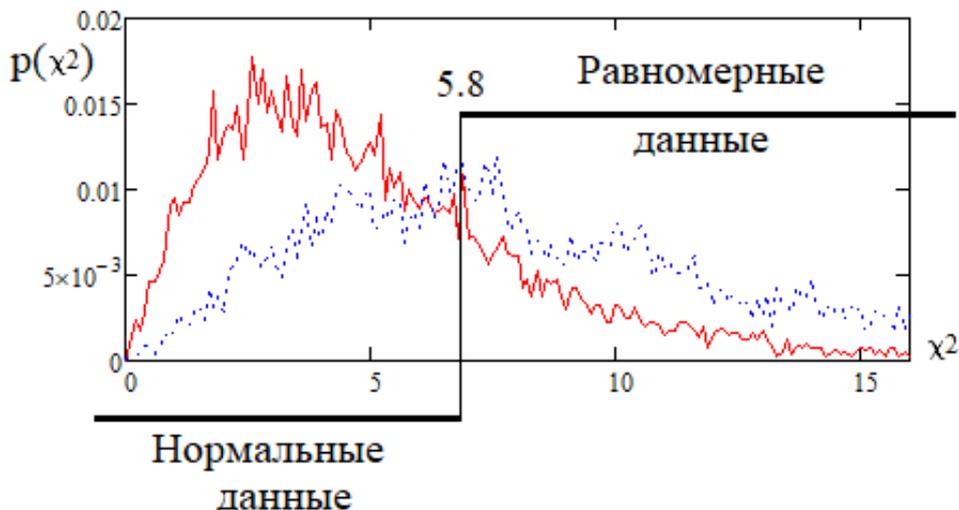


Рис. 17. Пример плохой линейной разделимости искусственным нейроном выходных состояний хи-квадрат критерия Пирсона для малых выборок в 16 опытов

Очевидным является то, что для малых выборок вероятности ошибок первого и второго рода велики $P_1 = P_2 = P_{EE} = 0,330$. В связи с этим по стандартным рекомендациям [38] для приемлемых значений доверительных вероятностей критерий хи-квадрат должен применяться для выборок в 200 и более опытов.

Примерно такая же ситуация возникает и для других классических статистических критериев [39]. На рис. 18 приведены данные для статистического критерия Крамера – фон Мизеса. Как и хи-квадрат критерий он дает на малых выборках неприемлемо большие значения вероятностей ошибок первого и второго рода $P_1 = P_2 = P_{EE} = 0,405$.

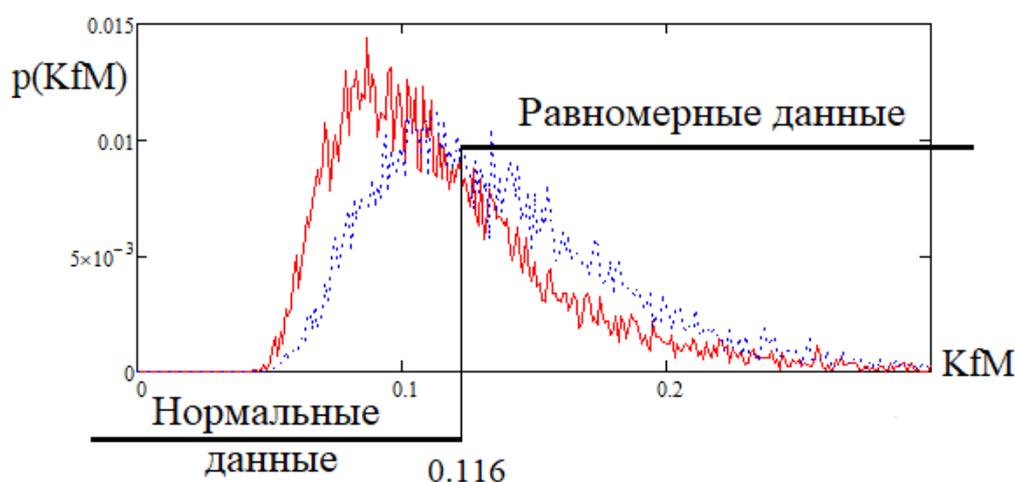


Рис. 18. Пример плохой линейной разделимости искусственным нейроном выходных состояний критерия Крамера – фон Мизеса (1928 г.) для малых выборок в 16 опытов

Равные вероятности ошибок первого и второго рода для нейрона Крамера – фон Мизеса возникают в случае, если пороговый элемент нейрона срабатывает при значении $k = 0,116$. При других значениях порога вероятности ошибок первого рода – P_1 (ошибочный отказ в признании гипотезы нормального распределения) и вероятности ошибок второго рода – P_2 (ошибочное отвержение гипотезы нормального распределения) не совпадают (между ними нет симметрии).

Синтез в 1928 г. статистического критерия Крамера – фон Мизеса дал математической общественности уверенность в том, что статистических критериев может существовать достаточно много. Начался активный поиск иных статистических критериев для проверки иных статистических критериев [39]. На протяжении XX в., усилиями специалистов по математической статистике, было создано порядка 200 статистических критериев, учитывающих те или иные особенности проверки статистических гипотез.

3.2. Нейросетевое обобщение классического критерия Смирнова – Крамера – фон Мизеса (1936 г.), Андерсона – Дарлингга (1952 г) и критерия Фроцини (1978 г.)

Тот факт, что синтезированный в 1928 г. критерий Крамера – фон Мизеса, имел мощность примерно на 30 % меньше, чем хи-квадрат критерий Пирсона, подстегнул многих исследователей. Как результат в 1936 г. был синтезирован критерий Смирнова – Крамера – фон Мизеса, мощность которого стала сопоставима с мощностью критерия Пирсона $P_1 = P_2 = P_{EE} = 0,320$. Распределения выходных состояний по этому модифицированному Смирновым критерию приведены на рис. 19.

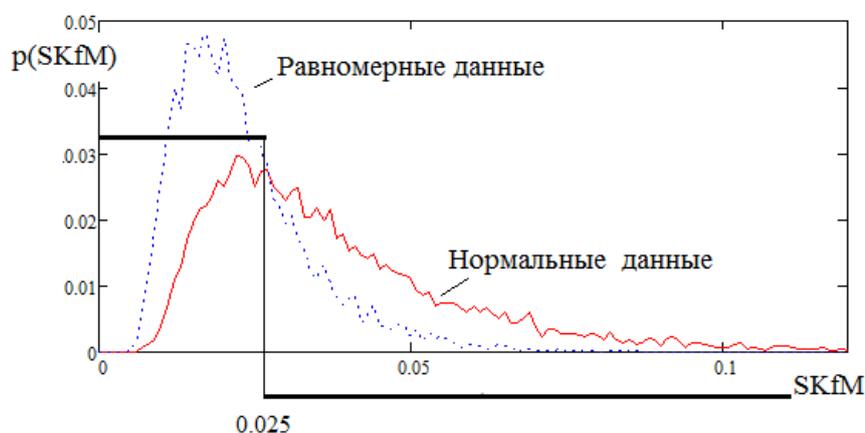


Рис. 19. Распределения выходных состояний НейроКритерия Смирнова – Крамера – фон Мизеса для выборки в 16 опытов

Программное обеспечение, написанное на языке MathCAD, численного эксперимента для получения данных (см. рис. 17–19) приведено в прил. 1.

Естественным желанием исследователей было получение статистического критерия, мощность которого была бы существенно выше мощности хи-квадрат критерия Пирсона. Такой критерий был создан Андерсоном и Дарлинггом в 1952 г., его выходные вероятностные состояния приведены на рис. 20.

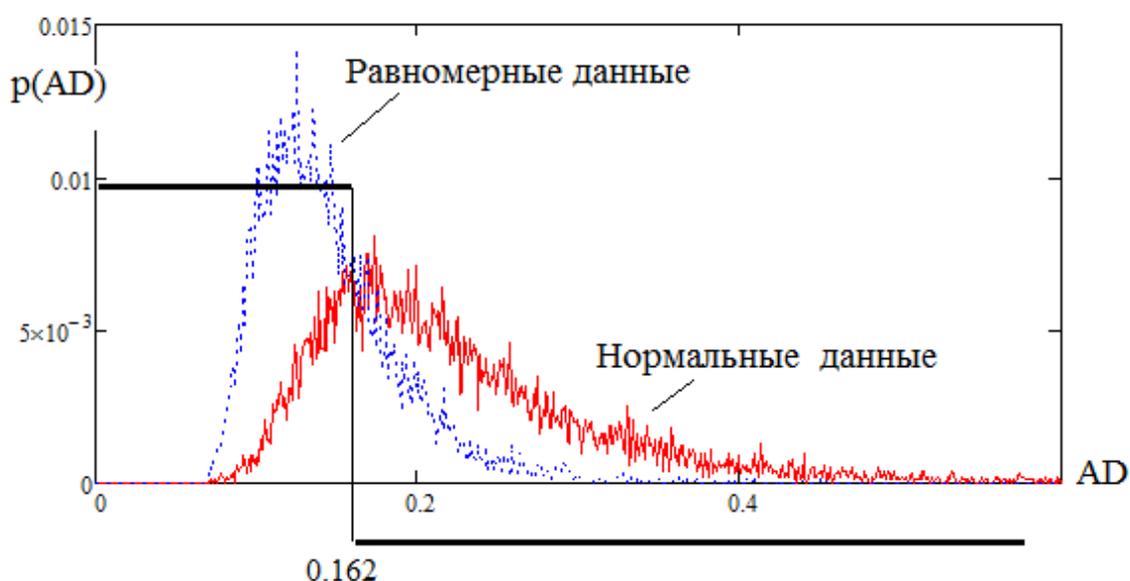


Рис. 20. Распределение выходных состояний НейроКритерия Андерсона – Дарлинга для малой выборки в 16 опытов

Статистический НейроКритерий Андерсона – Дарлинга уже обеспечивает $P_1 = P_2 = P_{EE} = 0,270$, что примерно на 20 % лучше в сравнении с хи-квадрат критерием Пирсона. Следующим шагом по повышению мощности статистических критериев проверки гипотезы нормальности является критерий Фроцини, созданный в 1978 г. Плотности вероятности выходных состояния критерия Фроцини для выборки, объемом в 16 опытов, приведены на рис. 21.

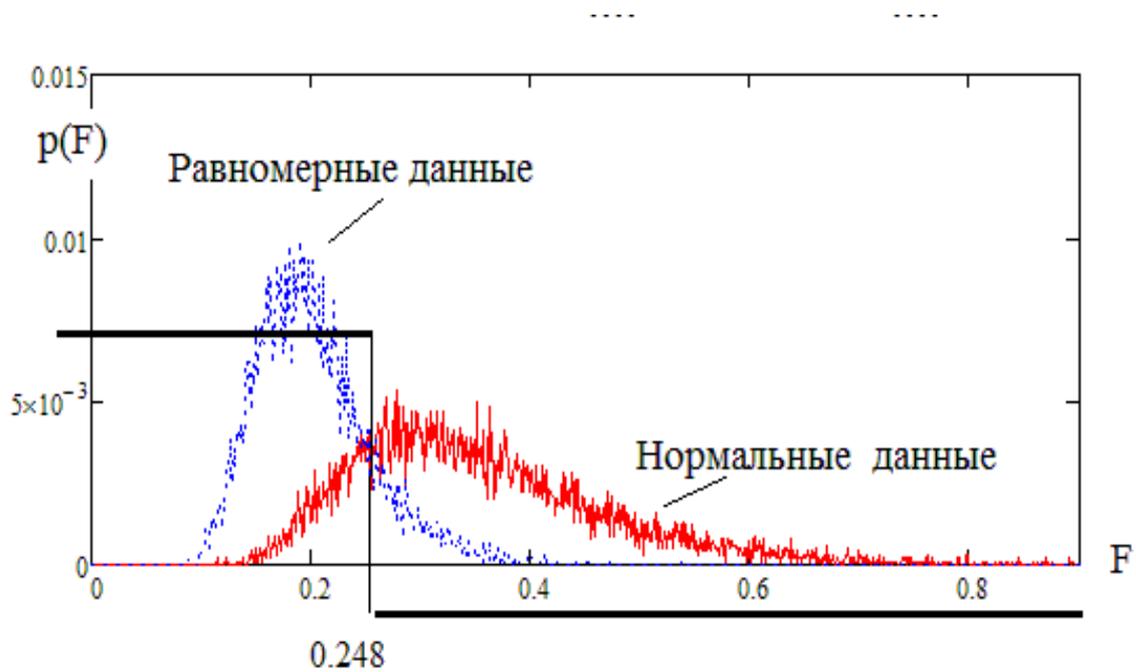


Рис. 21. Распределение выходных состояний НейроКритерия Фроцини для малой выборки в 16 опытов

Для этого статистического критерия вероятности ошибок первого и второго рода снижаются до величины $P_1 = P_2 = P_{EE} = 0,172$, что уже на 94 % лучше в сравнении с хи-квадрат критерием Пирсона.

3.3. НейроКритерии Муроты – Такеучи (1981 г.) и Васичека (1976 г.)

Еще одно заметное событие в теории статистических оценок произошло в 1976 г., когда был создан критерий Васичека. Этот критерий, видимо, имеет самую высокую мощность (минимальное значения равновероятных ошибок $P_1 = P_2 = P_{EE} = 0,06$. Плотности вероятности его выходных состояний при воздействии нормальными и равномерными данными приведены на рис. 22.

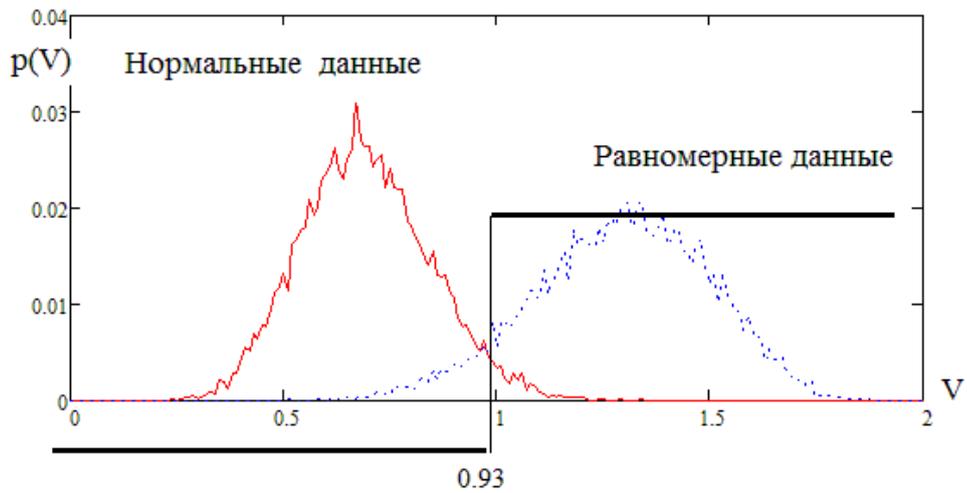


Рис. 22. Распределение выходных состояний наиболее мощного НейроКритерия Васичека для малой выборки в 16 опытов

Чуть меньшую мощность по разделению равномерных и нормальных данных имеет статистический критерий Муроты – Такеучи, синтезированный в 1981 г. Плотности распределения значений его выходных состояний отображены на рис. 23.

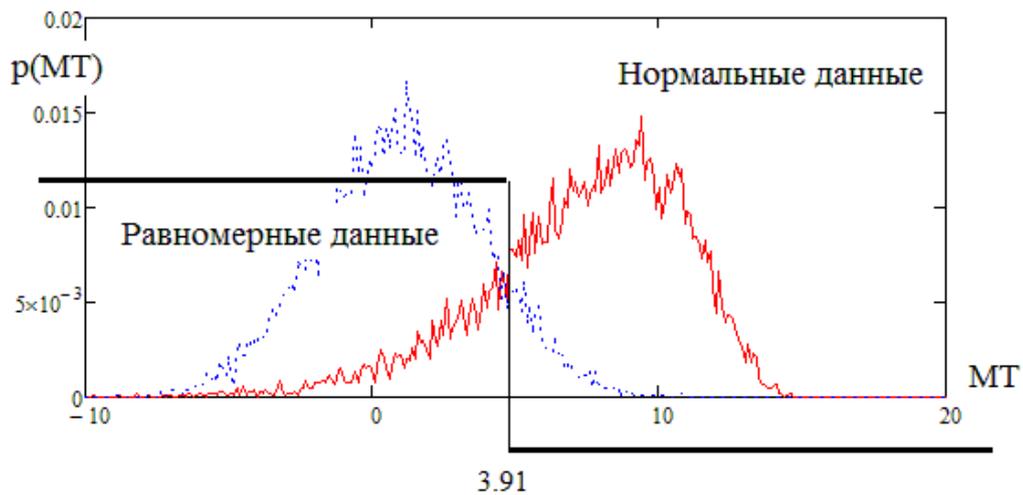


Рис. 23. Распределение выходных состояний НейроКритерия Муроты – Такеучи для малой выборки в 16 опытов

Получается, что в период с 1900 по 1981 г. лучшие исследователи последовательно создавали статистические критерии, обладающие все

большой и большей мощностью при проверке гипотезы нормального распределения той или иной выборки. За это время удалось снизить с вероятностей $P_1 = P_2 = P_{EE} = 0,330$ до вероятностей $P_1 = P_2 = P_{EE} = 0,06$ более чем в 5,5 раза. Если в начале XX в. мы могли принимать решения с доверительной вероятностью 0,67, то в конце века мы уже могли принимать решения с доверительной вероятностью 0,94 для малых выборок, объемом в 16 опытов.

3.4. Сеть из 21 искусственного нейрона, полученных обобщением 21 классического статистического критерия

В предыдущих разделах были рассмотрены семь классических статистических критериев и было показано, что каждому из них может быть поставлен в соответствие эквивалентный искусственный нейрон. Очевидно, что из этих 7 искусственных нейронов может быть собрана НейроСеть, которая будет иметь 7 выходов. Если все 7 выходов будут давать состояния «0000000», то с очень высокой вероятностью входная выборка будет иметь нормальный закон распределения. Если возникает другая ситуация, когда код состоит из единиц «1111111», то с высокой вероятностью можно говорить об обнаружении малой выборки с равномерным законом распределения значений.

В случае, когда в коде одновременно появляются и состояния «0», и состояния «1», приходится получать однозначное решение, используя теорию кодов с обнаружением и исправлением ошибок. Простейший такой код ориентирован на нечетное число разрядов и работает на подсчете числа состояний «0» и числа состояний «1». Если число нулей больше числа единиц, то принимается решение об обнаружении выборки с нормально распределенными данными.

Очевидно, что все коды с обнаружением и исправлением ошибок работают тем лучше, чем выше их избыточность. Если использовать 7 нейронов, то мы имеем 6-кратную избыточность кода. Однако, если использовать 21 классический статистический критерий (см. табл. № 80 с. 278 [40]), то мы получим 20-кратную кодовую избыточность. Естественно, что самокорректирующиеся коды с 20-кратной избыточностью будут работать лучше, чем с 6-кратной избыточностью. На рис. 23 представлена схема НейроСетевого обобщения хорошо исследованных на сегодня 21 статистических критериев.

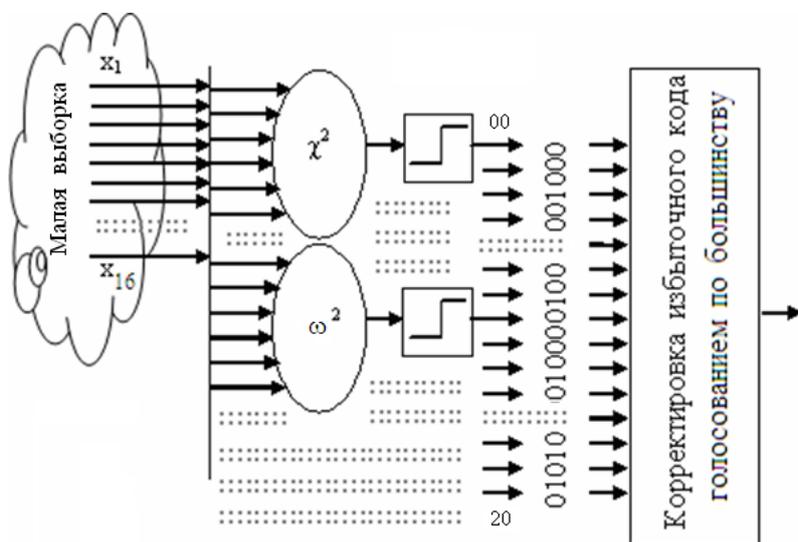


Рис. 23. Нейросетевое обобщение 21 классического статистического критерия

К сожалению, на текущий момент пока нет полноценного программного обеспечения, поддерживающего подобные НейроСетевые обобщения. Проблема упирается в поиск спонсоров под этот класс НейроСетевого программирования. Когда ищешь деньги, нужно уметь внятно объяснить, что должно получиться в конце проекта. Какова должна быть доверительная вероятность НейроСетевых решений, построенных с использованием всех 21 классических статистических критериев проверки гипотезы нормального распределения.

3.5. Симметризация НейроСетевых обобщений статистических критериев для учета значений их коэффициентов взаимной корреляции

Если мы остаемся в рамках линейной алгебры и пытаемся решать системы уравнений, то увеличение корреляционной связанности даже двух параметров приводит к катастрофическому росту коэффициента обусловленности. В нашем случае появление двух полностью коррелированных нейронов дает коды с двумя повторяющимися разрядами. Один разряд может быть отброшен.

В общем и целом приходится учитывать полную корреляционную матрицу учитываемых коэффициентов корреляции между выходными состояниями разрядов кода.

В связи с тем, что корреляционные матрицы симметричны, будем отображать только их правый треугольник, тогда корреляционная матрица, рассмотренная выше, семи искусственных нейронов будет выглядеть следующим образом:

$$[r] = \begin{bmatrix} 1 & 0,49 & 0,9 & 0,85 & 0,73 & 0,38 & -0,14 \\ & 1 & 0,34 & 0,46 & 0,12 & 0,25 & -0,08 \\ & & 1 & 0,95 & 0,93 & 0,56 & -0,41 \\ & & & 1 & 0,92 & 0,63 & -0,53 \\ & & & & 1 & 0,67 & -0,56 \\ & & & & & 1 & -0,16 \\ & & & & & & 1 \end{bmatrix} \Rightarrow . \quad (11)$$

Мы наблюдаем достаточно сильные корреляционные связи между выходными кодовыми состояниями нейросети. Пренебрегать столь значительными корреляционными связями нельзя. В связи с этим следует выполнить симметризацию корреляционных связей [41, 42]. Чем выше размерность корреляционной матрицы, тем точнее ее замена на эквивалентную симметричную матрицу с одинаковыми коэффициентами кор-

реляции вне диагонали. Вычисление одинаковых коэффициентов корреляции выполняется усреднением модулей всех коэффициентов корреляции, находящихся вне диагонали:

$$\tilde{r} = E\{|r_{i,j}|\} \quad \text{для } i \neq j. \quad (12)$$

Подобное усреднение для данных асимметричной корреляционной матрицы (11) дает следующую уже симметричную корреляционную матрицу

$$\Rightarrow [\tilde{r}] = \begin{bmatrix} 1 & 0,55 & 0,55 & 0,55 & 0,55 & 0,55 & 0,55 \\ & 1 & 0,55 & 0,55 & 0,55 & 0,55 & 0,55 \\ & & 1 & 0,55 & 0,55 & 0,55 & 0,55 \\ & & & 1 & 0,55 & 0,55 & 0,55 \\ & & & & 1 & 0,55 & 0,55 \\ & & & & & 1 & 0,55 \\ & & & & & & 1 \end{bmatrix}. \quad (13)$$

Процедура симметризации аналитически строго вводится в теории ядер Вольтера [43–47]. Для нейронных сетей столь строгого аналитического доказательства нет. Тем не менее, описанные выше преобразования симметризации хорошо подтверждаются практикой их применения.

Еще одним аспектом симметризации является устранение расхождения вероятностей ошибок первого и второго рода для разных нейронов. Эта процедура выполняется вычислением их среднего геометрического

$$\tilde{P}_{EE} \approx \sqrt[7]{P_{EE,1} \cdot P_{EE,2} \cdot P_{EE,3} \cdot P_{EE,4} \cdot P_{EE,5} \cdot P_{EE,6} \cdot P_{EE,7}} = 0,21. \quad (14)$$

Перейдя к симметризованной модели НейроСетивого обобщения, мы существенно облегчаем программирование численных экспериментов. В прил. 2 дана программа на языке MathCAD численного эксперимента, позволяющего убедиться в том, что «тупая» сборка всех известных классических статистических критериев и последующее ис-

пользование простейших кодов для обнаружения и исправления ошибок не дают положительного результата. Данные численного эксперимента отображены на рис. 24.

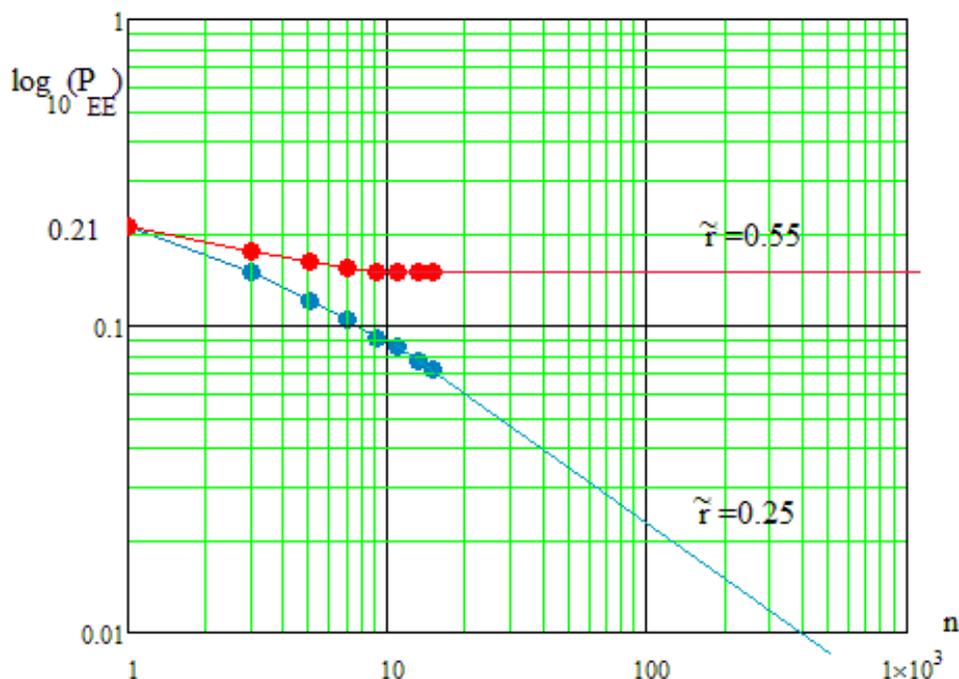


Рис. 24. Прогноз улучшения качества принимаемых НейроСетью решений при разном уровне корреляционной сцепленности данных

Из рис. 24 видно, что при уровне корреляционной сцепленности $\tilde{\gamma} = 0,55$ корректирующая способность простейших кодов быстро утрачивается. Они оказываются неспособны выполнять исправление ошибок уже при 10-кратной избыточности. Совершенно иная ситуация возникает, когда удастся снизить уровень корреляционной сцепленности до величины $\tilde{\gamma} = 0,25$. В этом случае мы наблюдаем монотонное снижение вероятностей ошибок с ростом избыточности простейшего кода, однако уровень снижения незначителен. Достигнуть приемлемого значения доверительной вероятности в 0,99 удастся только при использовании 400 статистических критериев. Проще взять один самый мощный статистический критерий Васичека, обеспечивающий уровень доверительной

вероятности 0,94, а все иные статистические критерии отбросить. Это популярная классика предыдущих столетий, когда исследователь пытается найти самые информативные параметры, а все остальные отбросить. Поиск наиболее информативных параметров [48, 49, 59] или выделение главных компонент – это поиск в прозрачном ручье золотых самородков (информационных самородков). Да, иногда их можно отыскать, но их очень мало. Нужно много времени, чтобы отыскать свой самородок или свою пару информационных самородков.

Гораздо более производительным является соорудить лоток и перейти к промывке золотого песка (информативного песка). От ручного поиска нужно переходить к созданию некоторой промышленной установки для обогащения относительно бедных данных. Информативных песчинок по совокупному информационному весу гораздо больше, чем информативных самородков. В предыдущем разделе было показано, что каждый из известных статистических критериев проверки статистической гипотезы нормальности распределения данных малых выборок, способен извлекать некоторую толику информации. Однако их совокупность обладает сильной корреляционной сцепленностью. Сильная корреляционная сцепленность мешает применению простейших кодов с обнаружением и исправлением ошибок. При высокой корреляционной сцепленности «сырых» данных не играет роли их объем. В этом отношении предпринимаемые сегодня попытки синтеза новых статистических критериев среднего геометрического [51–54], и новых статистических критериев среднего гармонического [53–56] могут оказаться бесполезными. При синтезе новых статистических критериев нужно обеспечить их низкую корреляционную сцепленность. Предположительно, это можно сделать, воспользовавшись полиномиальными ортогональными нейронами [57].

ГЛАВА ЧЕТВЕРТАЯ

ПЕРЕХОД ИЗ НЕЙРОСТАТИКИ В НЕЙРОДИНАМИКУ, ЗАМЕНА СТАТИСТИЧЕСКИХ НЕЙРОКРИТЕРИЕВ МАТЕМАТИЧЕСКИМИ МОЛЕКУЛАМИ

4.1. Наблюдение спектра амплитуд вероятности появления расстояний Хэмминга путем модуляции входных данных НейроСети через их случайное прореживание

Симметризация задачи нейросетевого обобщения статистических критериев проверки гипотезы нормальности в НейроСтатике показывает, что для ее решения с доверительной вероятностью приемлемой для практики потребуется к 21 классическому критерию добавить $(400 - 21) = 379$ дополнительно созданных статистических критериев. Если учесть, что в прошлом веке создано порядка 40 пригодных для этой цели статистических критериев, то нам на такую работу потребуется порядка 10 веков. Эта оценка затрат сверхху.

Оценку затрат снизу можно выполнить исходя из того, что г. Пенза примерно за 10 лет создала порядка 10 новых статистических критериев [51–56] среднего геометрического и среднего гармонического, т.е., одна кафедра в одном университете вполне способна синтезировать по одному новому статистическому критерию в год. В России сегодня существует порядка 1000 университетов, каждый из которых имеет хотя бы одну кафедру математики или математической статистики, т.е. этих сил вполне достаточно, чтобы общими усилиями разработать за один год 1000 новых статистических критериев.

Видимо, это было реально во времена планирования развития науки в СССР, для сегодняшней либерально-неуправляемой России – это утопия. Если этими задачами будет заниматься одна кафедра г. Пензы, то мы получим достаточное число статистических критериев при-

мерно через 300 лет. Столько ждать нельзя и нужно искать методы, которые позволят снизить затраты и время ожидания в несколько раз.

Одним из перспективных путей создания эффективных обогатителей информации является переход из НейроСтатики в НейроДинамику [58–61]. Находясь в НейроСтатике, на одну проверяемую малую выборку в 16 опытов мы получаем один выходной код. Естественно, что мы не видим амплитуд вероятности спектра линии расстояний Хэмминга. Однако, если мы возьмем нормальную выборку чуть больше, например, в 21 опыт, то мы сможем случайным образом выбирать по 5 опытов и отбрасывать их. В итоге мы можем получить

$$\frac{21!}{16!(21-16)!} = 20\,349$$

меньших подвыборок, отличающихся от друг друга хотя бы одним из 16 опытов. Вместо одной выборки мы получаем 20 000 подвыборок, что отображено на рис. 25.

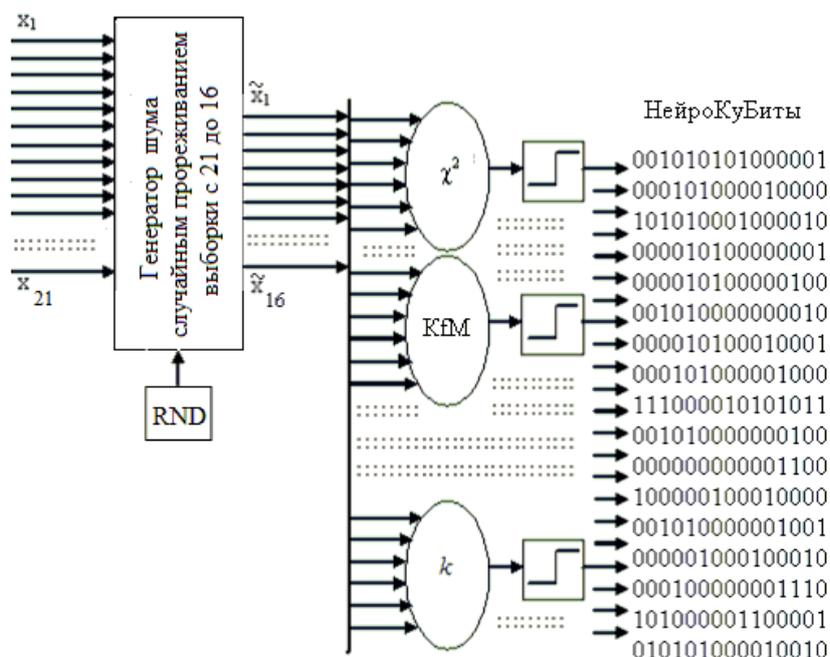


Рис. 25. Модуляция входных данных НейроСети прореживанием выборки, состоящей из 21 опыта случайным выбором и отбрасыванием 5 опытов

Очевидно, что уже в этой новой ситуации мы можем видеть спектральные линии амплитуд вероятности Хэмминга.

Реализация программного кода предварительного вычисления колоды из 64 карт случайного отбрасывания 5 номеров из выборки в 21 опыт приведена в прил. 3.

К сожалению, столь простого наблюдателя всего 8 спектральных линий расстояний Хэмминга оказывается недостаточно для существенного снижения вероятности ошибок принимаемых статистических решений. Описанных в данной работе 7 НейроСетевых обобщений недостаточно. Необходимо либо увеличивать число нейронов, либо НейроСеть нужно делать многослойной. Как следует из табл. 1, выигрыш в быстродействии и, видимо, выигрыш в повышении достоверности вычислений зависит от числа слоев нейронов или от числа выполненных итераций по переходу от континуального накапливания данных к их квантованию. Выигрыш в точности или в быстродействии как раз и происходит на границе перехода из континуумов в цифры.

Еще одной побочной проблемой НейроСтатики является огромное усложнение разработки программного обеспечения. В нашем случае получается, что НейроСтатика предполагает усложнение программного обеспечения в более чем в 400 раз. Вместо программной реализации одного хи-квадра критерия, объемом в 7 строк кода, потребуются реализовать программное воспроизведение 400 статистических нейронов. В этом отношении переход от НейроСтатики в НейроДинамику позволяет ощутимо уменьшить сложность программного обеспечения. Вполне возможно, что применение модуляторов данных случайным прореживанием (см. рис. 25) позволит вместо 400 статистических НейроКритериев использовать хотя бы 200 статистических НейроКритериев.

По схеме НейроМодуляции (см. рис. 25) одно и то же программное обеспечение запускается многократно и при этом получается неко-

торый выигрыш в качестве принимаемых нейросетевым искусственным интеллектом решений. Всегда проще написать и отладить одну маленькую менее сложную программку, а потом ее многократно использовать в сравнении одной большой сложной программой, предназначенной к ее однократному запуску.

При этом следует отметить, что число анализируемых спектральных линий всегда на единицу больше, чем число реализованных программно НейроКритериев. Возникает резонный вопрос о том, можно ли изменить это соотношение. Возможна ли ситуация получения на выходе некоторой математической конструкции с вычислительной сложностью одного НейроКритерия, но более сложным (много линейчатым) выходным дискретным спектром.

4.2. Математическая хи-квадрат молекула

В 1900 г. Пирсон создал хи-квадрат критерий проверки статистических гипотез. Критерий Пирсоном строится, опираясь на гистограмму, отображенную в левой части рис. 26.

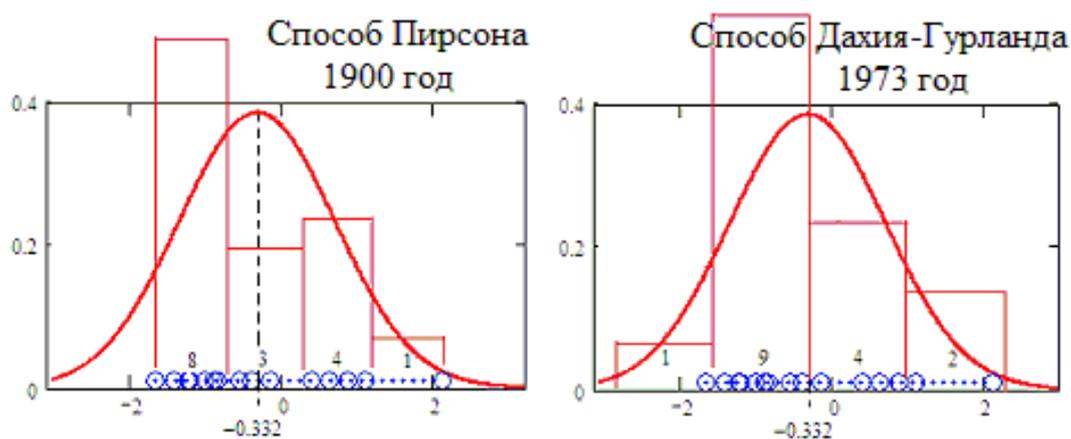


Рис. 26. Два разных способа построения гистограмм для выборки в 16 опытов

Сегодня считается, что хи-квадрат критерий надежен на выборках в 200 и более опытов. Однако столь большую выборку не всегда удается

получить на практике. Так, биолог далеко не всегда может провести 200 измерений, интересующего его параметра у 200 подопытных животных, получив высокую достоверность оценок. Если же он выполнит только 16 опытов, то доверительная вероятность его оценок по хи-квадрат критерию оказывается неприемлемо низкой.

Иллюстрацией низкого качества решений, принимаемых критерием Пирсона на малых выборках, служит рис. 17. С позиций сегодняшнего дня становится понятным причина низкого качества принимаемых решений. Пирсон в 1900 г. использовал не самый удачный способ формирования гистограмм, приводящий к наблюдению непрерывных распределений. Пирсон не принимал во внимание положение математического ожидания исследуемой выборки.

Если мы изменим способ формирования гистограмм, как это сделали Дахия и Гурланд [62] в 1973 г., то получим дискретный спектр разрешенных выходных состояний дискретного хи-квадрат критерия. По новому способу математическое ожидание исследуемой выборки всегда попадает точно в цент формируемой гистограммы.

Так же, как молекула водорода имеет выходной дискретный спектр линий светимости или поглощения, вариант формирования столбцов гистограммы 1973 г. дает только дискретные (разрешенные) выходных состояний хи-квадрат критерия. В этом отношении хи-квадрат критерий Пирсона можно рассматривать как некоторую математическую молекулу, возбуждаемую либо малыми выборками нормальных данных либо малыми выборками данных, с равномерным распределением.

Программное обеспечение для численного моделирования дискретной хи-квадрат молекулы Пирсона дано в прил. 4. Результаты численного моделирования отображены на рис. 26.

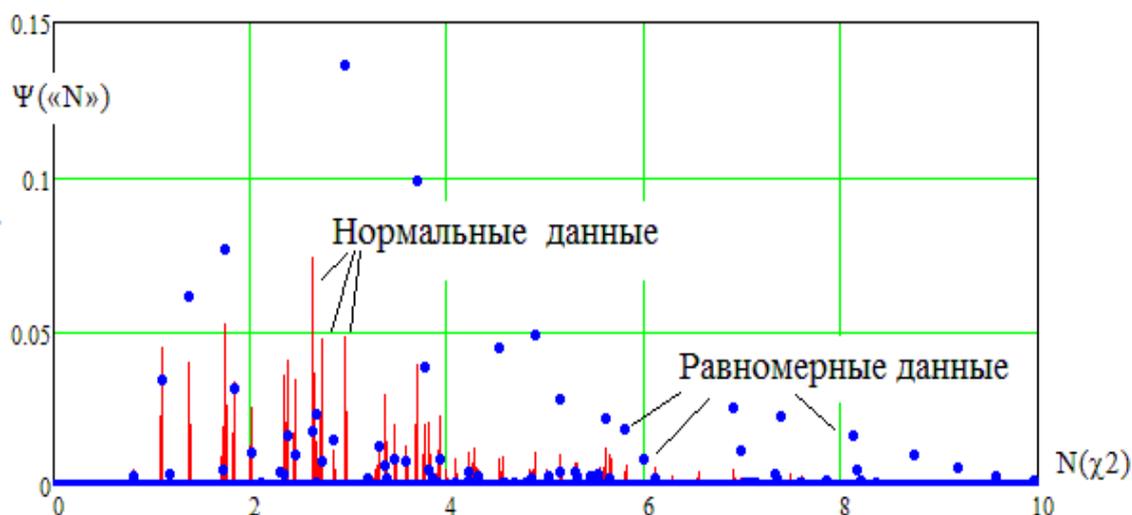


Рис. 26. Результаты численного моделирования дискретной хи-квадрат молекулы Пирсона, возбуждаемой малыми выборками в 16 опытов

Сравнивая рис. 17 с распределением непрерывного хи-квадрат критерия и дискретного хи-квадрат критерия рис. 26, мы наблюдаем принципиальные различия между ними. Между разрешенными выходными состояниями хи-квадрат молекулы с достаточно большим амплитудами вероятности $\Psi(«N»)$ наблюдаются значительные интервалы невозможных (запрещенных) состояний. Мощность континуального спектра обычного хи-квадрат распределения (см. рис. 17) по некоторому интервалу стягивается в точку той или иной спектральной линии. Именно это обстоятельство и дает потенциальную возможность перейти от обычной континуально-спектральной статистической обработки к квантовым методам статистического анализа.

Следует отметить, что на момент обнаружения эффектов квантования выходных состояний хи-квадрат молекулы Дахия и Гурланд в 1973 г. [62] не оценили его значимости. Открытие скорее удивило его авторов, чем обрадовало. Как-то использовать новый эффект авторы открытия даже не пытались. Дело в том, что на тот момент не было известно об огромных преимуществах квантовых вычислений. Юрий Ма-

нин предложил использовать эффекты квантовой суперпозиции только через 7 лет [30], в 1980 г., а математически строгие обоснования подобных возможностей были сделаны намного позже [31–33]. Повторное обнаружение возможности перехода к дискретному спектру хи-квадрат критерия [63] было выполнено в 2015 г. Тогда для специалистов были очевидны перспективы применения дискретных спектров для реализации квантовых вычислений [65, 66].

Следует также отметить, что одной из особенностей спектров амплитуд вероятности $\Psi(\langle N \rangle)$ хи-квадрат молекулы является совпадение спектральных линий для малых выборок с равномерным и нормальным распределением. Спектры различаются между собой только амплитудами вероятности, что отображено в табл. 2 для первых 19 спектральных линий.

Таблица 2

Амплитуда вероятности

N	0	1	2	3	4	5	6	7	8	9
Ψ_r	32	356	32	605	0	42	727	0	0	341
Ψ_n	50	407	82	421	1	187	517	2	5	358
χ^2	0.82	1.1	1.19	1.39	1.44	1.73	1.76	1.81	1.82	1.84

N	10	11	12	13	14	15	16	17	18	19
Ψ_r	90	5	2	29	38	140	116	4	749	116
Ψ_n	279	19	11	26	296	388	351	4	6	749
χ^2	2.01	2.1	2.28	2.31	2.36	2.38	2.46	2.55	2.63	2.65

Следует отметить, что приведенные выше амплитуды вероятности вычислены программой прил. 3 и их значения являются завышенными примерно в 10 000 раз.

Параллельно с распределением линий спектра амплитуд вероятностей (см. рис. 26) мы можем проинтегрировать это распределение, получив две функции вероятности, приведенные на рис. 27.

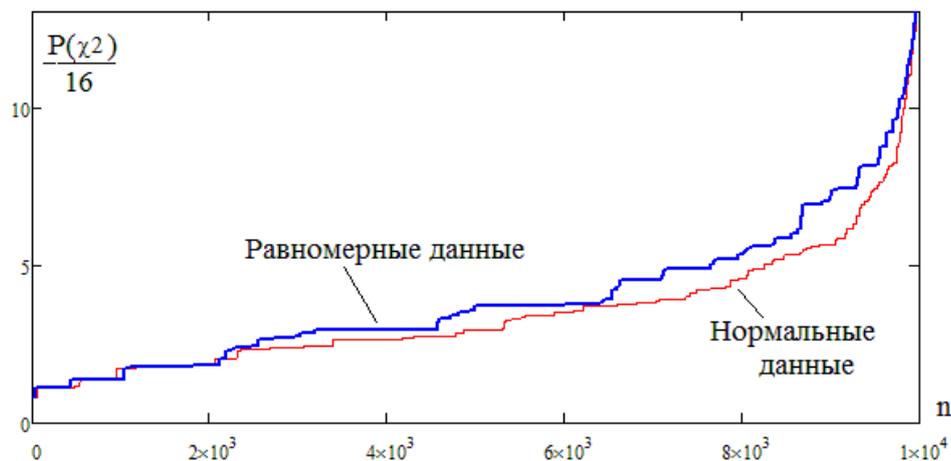


Рис. 27. Функции вероятности, полученные интегрированием (накапливанием) амплитуд вероятностей разнесенных между собой спектральных линий $\Psi(\langle\chi^2\rangle)$, представленных на предыдущем рис. 26

Следует отметить, что число ровных площадок на графиках рис. 27 примерно одинаково для нормальных данных и равномерно распределенных данных, т.е. значимых спектральных линий с достаточно высокой амплитудой вероятности для рассматриваемых распределений сопоставимо. Спектральных линий с малой амплитудой вероятности намного больше для нормальных данных, особенно для больших значений хи-квадрат критерия.

Следует также отметить, что подобно хи-квадрат молекуле математические конструкции уже построены для критериев среднего геометрического [65] и среднего гармонического. Кроме того, большая часть классических статистических критериев для проверки гипотезы независимости малых выборок уже являются статистическими молекулами [66–68]. Таким образом, на сегодняшний день НейроДинамику в контексте получения повышения достоверности принимаемых статистических решений сетями НейроКритериев скорее всего следует рассматривать не как самостоятельное направление исследований, а как метод упрощения программирования, позволяющий многократно применять упрощенные в два и более раз программные реализации.

4.3. Интеллектуализация автоматического алгоритма обучения сетей искусственных нейронов на малых обучающих выборках

4.3.1. НейроСетевое предсказание ошибок вычисления математического ожидания и стандартного отклонения на малых выборках с нормальным распределением данных

Алгоритм автоматического обучения НейроСетей по ГОСТ Р 52633.5 построен на знании математического ожидания малых выборок БиоДанных образа «Свой». Предположим, что оцениваемый биометрический параметр имеет нулевое математическое ожидание, однако мы этого не увидим. Из-за использования малой выборки в 16 опытов мы можем получить ошибку оценки матожидания, лежащую в интервале от -1 до $+1$, как это показано на рис. 28.

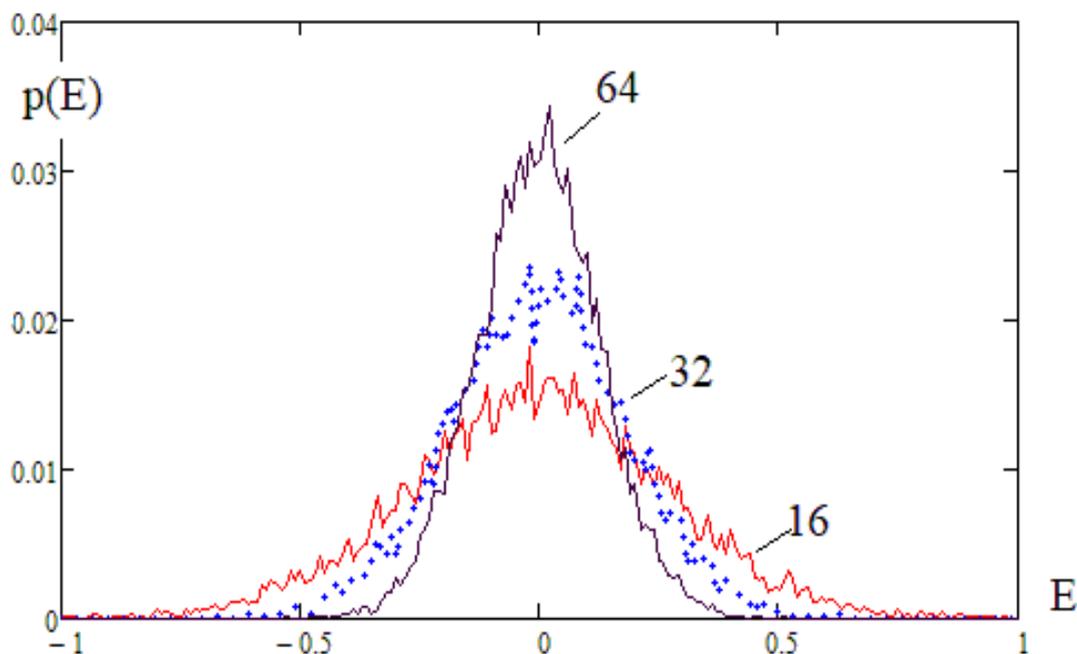


Рис. 28. Распределение значений математических ожиданий для малых выборок в 16, 32, 64 опыта с нормальным законом распределения значений после его нормирования (исходные данные получены от программного генератора с $E = 0,0$)

Получается, что мы имеем интервал неопределенности от $-0,7$ до $+0,7$ при оценке эталонных значений $E = 0,0$ на малых выборках в 16 опытов. Это огромный интервал возможных ошибок, однако алгоритм обучения ГОСТ Р 52633.5 дает устойчивые в вычислительном отношении процедуры НейроСетевой обработки биометрических данных. В частности, одной из причин повышения устойчивости (снижения чувствительности к ошибкам ΔE) является накопление данных путем их весового суммирования по всем входам нейрона. Весовое суммирование ослабляет влияние ошибок оценки математических ожиданий биометрических параметров, тем не менее, всегда желательно эти ошибки снизить. Это вполне реализуемо, если есть возможность увеличить объем обучающей выборки с 16 до 32 или до 64 опытов.

В биометрии это вполне реализуемо, но рост объема примеров, на которых НейроСеть обучается, негативно воспринимается пользователями. Производители средств биометрической аутентификации стремятся снизить требования к объему обучающей выборки, исходя из эргономики применения их средств биометрической защиты.

В ряде НейроСетевых приложений экономики [69] или биологии нередки ситуации, когда увеличить объемы обучающей выборки технически очень сложно. Так, если биолог (зоотехник) получил новую перспективную ветвь кроликов (уже имеет 16 взрослых кроликов), то увеличить их популяцию в два-четыре раза он сможет только через 6 месяцев. Можно ждать 6 месяцев и кормить более чем 16 взрослых кроликов, а можно попытаться предсказать статистический результат, включая и предсказание ошибки вычисления математического ожидания ΔE на уже имеющейся малой выборке. Общая структура НейроСетевого предсказателя ожидаемой ошибки при вычислениях из-за малого объема выборки представлена на рис. 29.

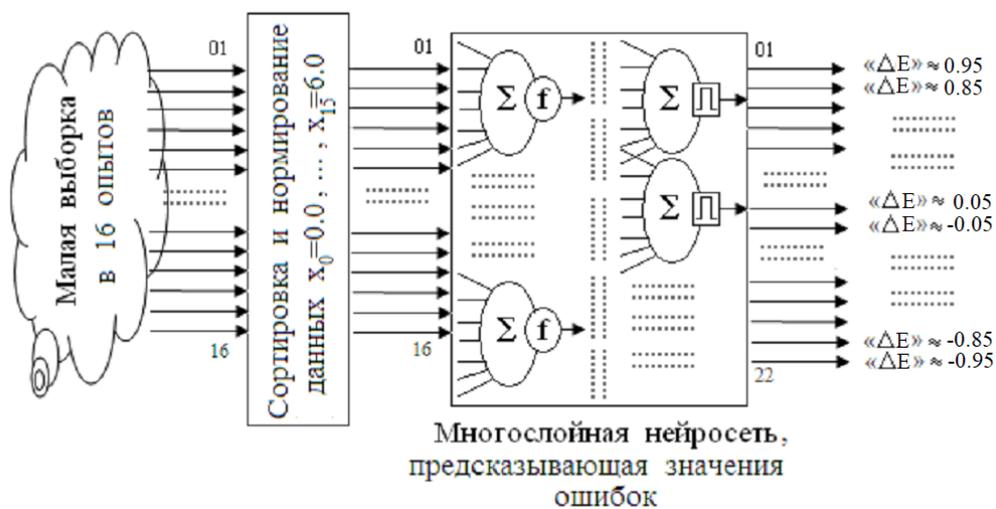


Рис. 29. НейроСетевой предсказатель ошибок вычисления математического ожидания на малых выборках в 16 опытов

Следует отметить, что для предсказания ошибок вычислений математического ожидания ΔE однослойные и двухслойные сети быстрого обучения алгоритмом ГОСТ Р 52633.5 использовать нельзя. Приходится использовать многослойные сети очень медленного обучения [70, 71]. Время обучения таких многослойных сетей не нормируется и быстро увеличивается по мере числа слоев нейронов в них. Для обучения «глубоких» многослойных сетей искусственных нейронов обычно требуется об миллионы примеров, если нам требуется различать «глубокой» сетью искусственных нейронов 22 класса с некоторой приемлемой ошибкой перепутывания двух соседних классов (например, на уровне $P_2 \approx 0,2$), то потребуется обучающая выборка, состоящая как минимум из 22 млн примеров. К счастью, получить подобные обучающие выборки от программных генераторов псевдослучайных чисел с нормальным распределением несложно.

Работа по синтезу НейроСетевых оракулов, заранее обученных предсказывать ошибки вычисления математических ожиданий для нормально распределенных выборок, начата в 2017 г. [72, 73]. На начало 2021 г. удалось достигнуть результатов, приведенных в табл. 3.

Снижение стандартного отклонения оценки математического ожидания при использовании НейроСетевого корректора ошибок и рост объема эквивалентной выборки для нормально распределенных данных

Число опытов	16		17		18		20	
Эталон	0,0	1,0	0,0	1,0	0,0	1,0	0,0	1,0
E(E)	0,0	1,0	0,0	1,0	0,0	1,0	0,0	1,0
E(E'')	-0,03	1,02	0,04	1,05	0,01	0,98	0,00	0,99
$\sigma(E)$	0,254	0,255	0,242	0,242	0,236	0,236	0,226	0,226
$\sigma(E'')$	0,166	0,156	0,157	0,159	0,154	0,155	0,148	0,149
Число опытов	34,1		36,5		39,4		42,2	

Таким образом, НейроСетевое предсказание ошибок вычисления математического ожидания для нормально распределенных данных позволяет примерно удвоить обучающую выборку или снизить интервал неопределенности примерно в полтора раза.

Кроме повышения точности вычисления математического ожидания на малых выборках совершенно такая же задача и при вычислении стандартных отклонений. Распределения значений стандартных отклонений для малых выборок приведены на рис. 30.

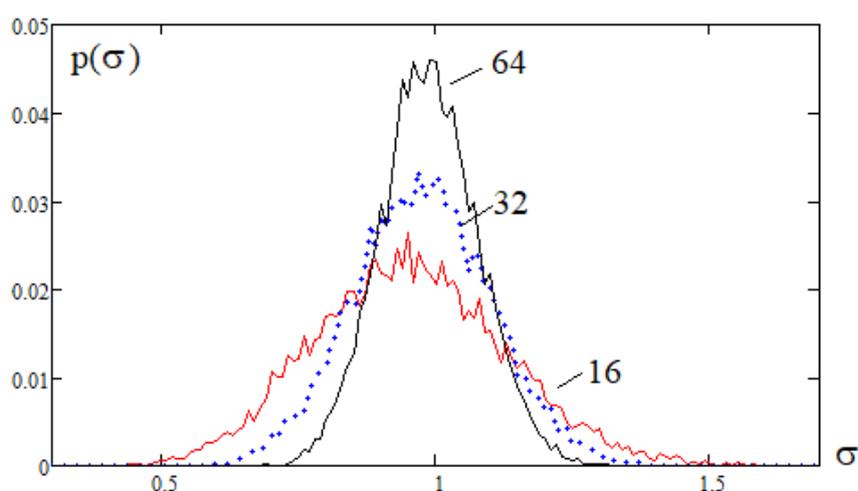


Рис. 30. Распределение значений стандартных отклонений для малых выборок в 16, 32, 64 опыта (нормальный закон распределения); исходные данные получены от программного генератора с $\sigma = 1,0$

Из рис. 30 видно, что проблема предсказания значений ошибок стандартных отклонений должна решаться не только с учетом интервалов неопределенности, но и учитывать их сдвиг относительно друг друга, т.е. нужно учитывать не только случайную составляющую погрешности, но и ее методическую составляющую. Если заранее компенсировать методическую погрешность [74], то мы приведем задачу нейросетевого прогноза ошибок стандартного отклонения к предыдущей задаче. В этом плане в НейроСеть предсказателя ошибок стандартного отклонения, подобную НейроСети на рис. 29, достаточно добавить блок компенсации методических ошибок (табл. 4).

Таблица 4

Повышение точности оценки стандартного отклонения при использовании нейросетевого корректора ошибок и рост объема эквивалентной выборки для нормально распределенных данных

Число опытов	16		17		18		20	
	1,0	2,0	1,0	2,0	1,0	2,0	1,0	2,0
Эталон	1,0	2,0	1,0	2,0	1,0	2,0	1,0	2,0
$E(\sigma)$	0,97	1,91	0,97	1,92	0,97	1,92	0,965	1,93
$E(\sigma'')$	1,01	1,99	0,99	2,04	1,00	1,99	0,99	1,99
$\sigma(\sigma)$	0,177	0,351	0,174	0,339	0,166	0,332	0,160	0,313
$\sigma(\sigma'')$	0,131	0,290	0,127	0,254	0,121	0,247	0,116	0,227
Число опытов	33,1	33,3	35,1	35,6	37,7	37,9	41,0	

Если сравнить данные двух последних таблиц, то становится очевидным близость достигнутых результатов. Это обусловлено тем, что в обоих случаях использовались глубокие НейроСети с одинаковой архитектурой и одинаковым числом слоев нейронов. Предположительно рост числа нейронов в слоях и рост числа слоев НейроСети будет приводить к повышению достоверности, принимаемых решений. Однако при этом экспоненциально растет сложность процедур обучения, также должен расти объем обучающей выборки.

Еще одним важным аспектом является то, что пока удастся выполнить обучение нейронных только для конкретного объема малых выборок, т.е. для формирования приведенных выше таблиц пришлось создавать и обучать 8 сетей искусственных нейронов.

4.3.2. НейроСетевая интеллектуализация автоматического алгоритма обучения сетей корреляционных нейронов Байеса

На текущий момент только в России введен в действие национальный стандарт автоматического обучения сетей искусственных нейронов с накоплением данных в линейном пространстве. Мировое сообщество пока не имеет международных стандартов по быстрому автоматическому обучению нейронных сетей на малых выборках.

Известно, что нейроны с накоплением данных в линейном пространстве хуже выделяют образы «Свой», размещенные внутри большей области «Все Чужие» [75, 76]. Эта ситуация отображена на рис. 31.

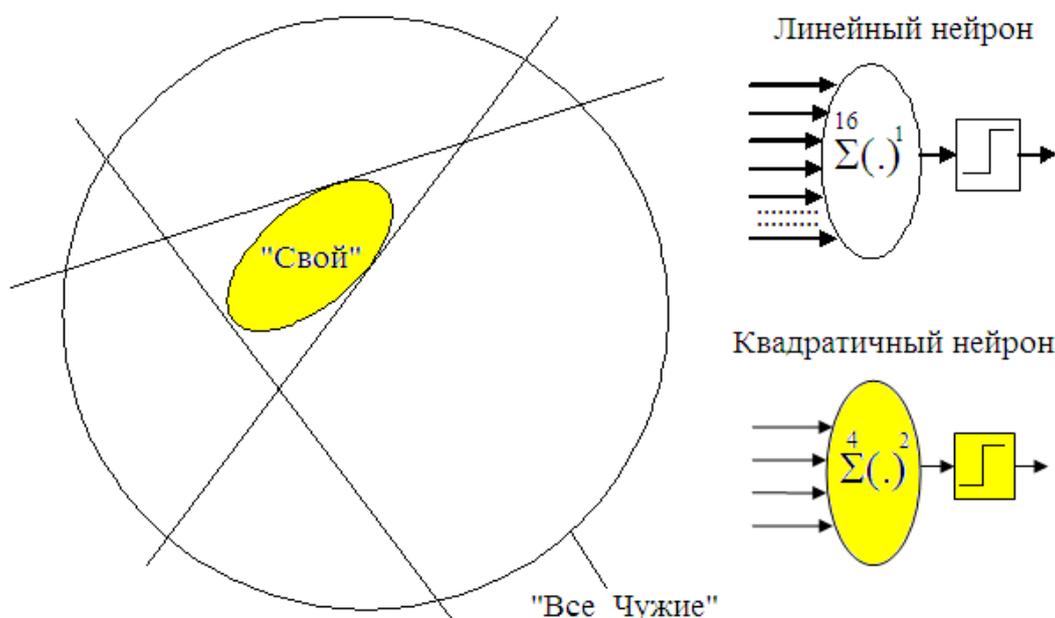


Рис. 31. Один квадратичный нейрон с эллиптической границей квантователя данных эквивалентен по своей эффективности примерно трем-четырем линейным нейронам

В связи с этим в России в настоящее время разрабатывается проект второго национального стандарта по устойчивому автоматическому обучению сетей квадратичных нейронов с многоуровневым квантованием [77]. Также разрабатывается третий национальный стандарт России по автоматическому обучению сетей корреляционных нейронов Байеса [78, 79].

Одной из проблем обучения квадратичных нейронов является корректное вычисление коэффициентов корреляции на малых выборках. Распределение значений коэффициентов корреляции, вычисленных на малых обучающих выборках, приведены на рис. 32.

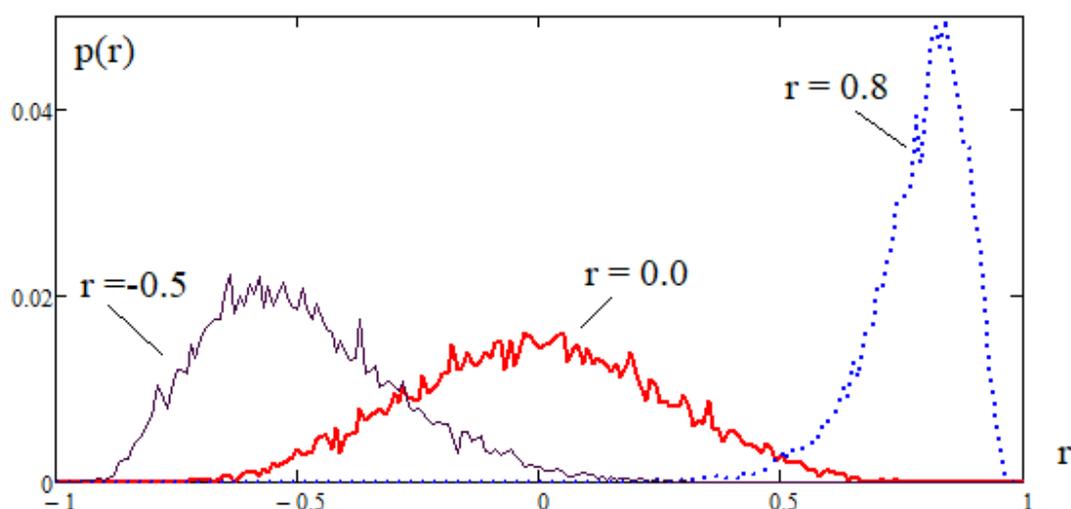


Рис. 32. Распределение значений коэффициентов корреляции двух малых выборок по 16 опытов (нормальный закон распределения); исходные данные получены от программного генератора $r = -0,5, r = 0,0, r = 0,8$

Из рис. 32 видно, что наибольшей проблемой является вычисление малых значений коэффициентов корреляции (проверка гипотезы независимости малых выборок [66]). Когда данные слабо зависимы $r = 0,0$, получается наибольший интервал неопределенности при вычислениях коэффициентов корреляции. Если модуль вычисляемого коэффициента корреляции увеличивается, то интервал неопределенности результата

вычислений сужается. В предельных ситуациях $r \rightarrow \pm 1,0$ неопределенность вычислений становится практически нулевой $\Delta r \rightarrow 0,0$.

Тем не менее и в этом случае необходимо предсказывать ошибки вычисления коэффициентов корреляции и далее по ним корректировать результаты классических вычислений. Работы по снижению погрешностей вычисления коэффициентов корреляции на малых выборках ведутся с 2016 г. силами одного-двух аспирантов. На текущий момент усилиями Ю. И. Сериковой [67, 74, 80] и Т. А. Золотаревой [66, 81–83] создано несколько новых статистических критериев проверки гипотезы независимости малых выборок. Однако сил для решения этой задачи было явно недостаточно. Уже созданные НейроСетевые корректоры ошибок работают намного хуже чем НейроСетевые корректоры ошибок вычисления математического ожидания и стандартного отклонения. Скорее всего, государственное финансирование этого направления работ усилится после разработки и введения в действие на территории РФ второго [77] и третьего [78, 79] национальных стандартов по автоматическому обучению сетей квадратичных нейронов на малых выборках.

С высокой вероятностью можно предсказать, что, скорее всего, будут развиваться НейроСети, построенные на основе НейроКритериев проверки гипотезы независимости малых выборок [66]. При этом, видимо, много НейроКритериев с достаточно независимыми откликами создать будет сложно [81], однако объем данных может быть существенно увеличен путем модулирования входных данных случайным прореживанием. В связи с этим на рис. 33 приведена блок-схема преобразования, построенная на использовании пяти НейроКритериев.

Наиболее эффективным НейроКритерием является классический:

$$r(x, y) = \frac{1}{16} \sum_{i=1}^{16} \frac{(E(x) - x_i) \cdot (E(y) - y_i)}{\sigma(x) \cdot \sigma(y)}. \quad (15)$$

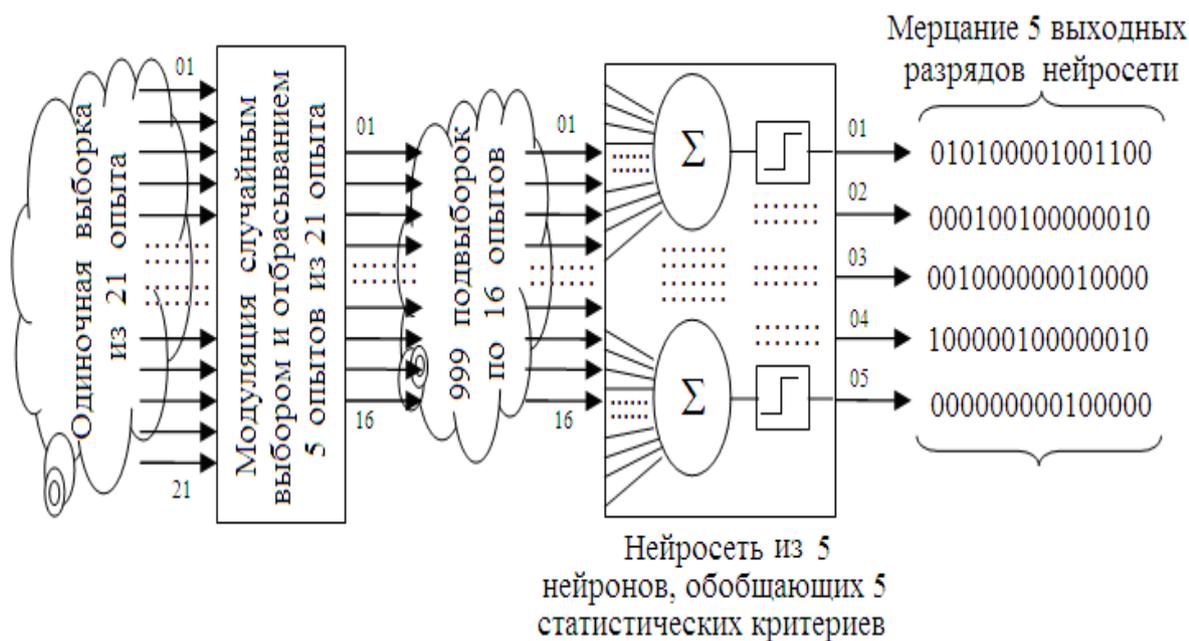


Рис. 33. Переход в НейроДинамику путем использования выборки в 21 опыт, случайного выбора пяти опытов и отбрасывания их из исходной выборки

К базовому, классическому НейроКритерию (11) могут быть добавлены четыре новых критерия:

$$\tilde{r}_0(x, y) = \frac{1}{16} \sum_{i=1}^{16} \frac{(E(x) - x_i) \cdot (E(y) - y_i)}{(E(x) - x_i)^2 + (E(y) - y_i)^2}; \quad (16)$$

$$\tilde{r}_1(x, y) = \frac{1}{16} \sum_{i=1}^{16} \frac{(\min(x) - x_i) \cdot (\min(y) - y_i)}{(\min(x) - x_i)^2 + (\min(y) - y_i)^2}; \quad (17)$$

$$\tilde{r}_2(x, y) = \frac{1}{16} \sum_{i=1}^{16} \frac{(\min(x) - x_i) \cdot (\max(y) - y_i)}{(\min(x) - x_i)^2 + (\max(y) - y_i)^2}; \quad (18)$$

$$\tilde{r}_3(x, y) = \frac{1}{16} \sum_{i=1}^{16} \frac{(\max(x) - x_i) \cdot (\max(y) - y_i)}{(\max(x) - x_i)^2 + (\max(y) - y_i)^2}. \quad (19)$$

Работоспособность НейроСети из пяти НейроКритериев подтверждается низкой корреляционной сцепленностью их выходных данных (табл. 5).

Статистические параметры нейросетевого обобщения пяти критериев

Формула	$P_1 \approx P_2$	Матрица коэффициентов корреляции					
		Формула	r (1)	\tilde{r}_0 (2)	\tilde{r}_1 (3)	\tilde{r}_2 (4)	\tilde{r}_3 (5)
r (15)	0,146	r (15)	1	0,75	0,338	0,344	0,316
\tilde{r}_0 (16)	0,211	\tilde{r}_0 (16)	0,75	1	0,317	0,324	0,295
\tilde{r}_1 (17)	0,334	\tilde{r}_1 (17)	0,338	0,317	1	-0,17	0,089
\tilde{r}_2 (18)	0,395	\tilde{r}_2 (18)	0,344	0,324	-0,17	1	-0,192
\tilde{r}_3 (19)	0,328	\tilde{r}_3 (19)	0,316	0,295	0,089	-0,192	1

Среднее геометрическое значение вероятностей ошибок первого и второго рода составляет $P_1 \approx P_2 \approx 0,271 \approx \sqrt[5]{0,146 \cdot 0,211 \cdot 0,334 \cdot 0,395 \cdot 0,328}$.

Среднее модулей коэффициентов корреляции составляет 0,36. Соотношения этих показателей достаточно для работоспособности НейроСетевого обобщения с блок-схемой (см. рис. 33).

4.4. Необходимость компенсации блужданий, возникающих при попытках вычислений младших статистических моментов на больших выборках

Сегодня в теории обучения сетей искусственных нейронов господствует убеждение, что рост объема обучающей выборки обязательно должен приводить к качеству обучения больших нейронных сетей. Появление первого в мировой практике стандарта по автоматическому обучению ГОСТ Р 52633.5 принесло серьезные сомнения в этой парадигме. Для обучения нужно знать математические ожидания и стандартные отклонения биометрических параметров. К сожалению, рост объема обучающей выборки с 20 до 1000 примеров необязательно приводит к пропорциональному росту точности оценок младших статистических моментов. К сожалению, при вычислениях статистических моментов возникает эффект блуждания, что отражают рис. 35, 36.

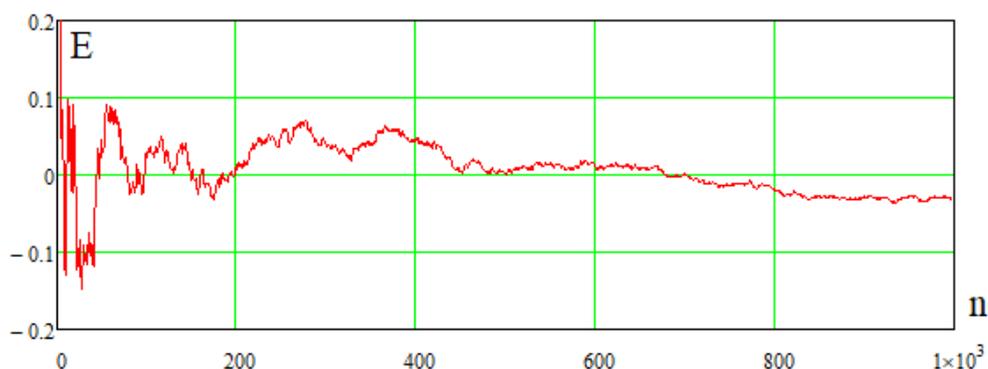


Рис. 35. Блуждания значений математических ожиданий, возникающие при монотонном увеличении объема выборки до 1000 опытов

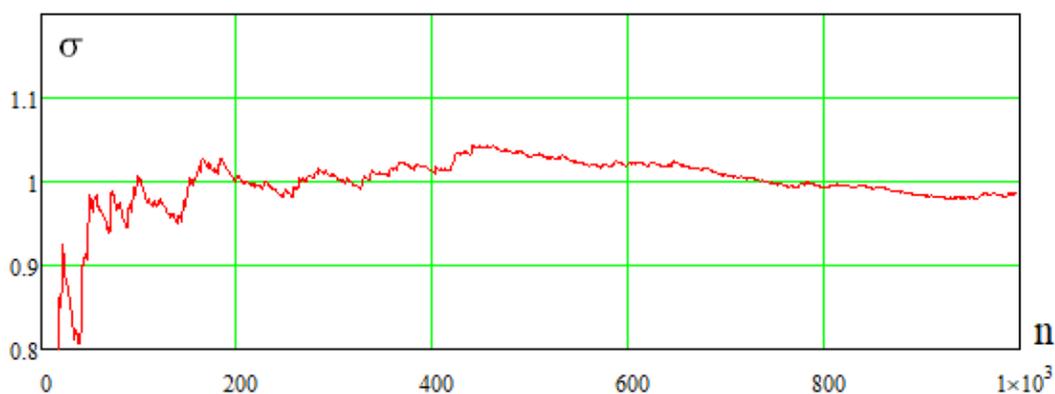


Рис. 36. Блуждания значений стандартных отклонений, возникающие при монотонном увеличении объема выборки до 1000 опытов

Если бы наблюдалось монотонное снижение ошибок вычисления статистических моментов, то можно было бы ожидать монотонного роста качества обучения. Случайное блуждание значения ошибок вычислений статистических моментов, видимо, должно приводить и к случайному блужданию качества обучения больших сетей искусственных нейронов. Это очевидно для неитерационного алгоритма обучения по ГОСТ Р 52633.5, однако это может быть также и для любых иных итерационных алгоритмов обучения.

Видимо, рассмотренные в данной работе алгоритмы НейроСетевой коррекции ошибок вычисления ошибок младших статистических

моментов на малых выборках будут весьма актуальны и для алгоритмов обучения и тестирования НейроСетей на больших выборках. Формально эффект блужданий при вычислении младших статистических моментов следует учитывать при применении международного стандарта [84] по тестированию биометрии. Приложение «В» этого стандарта содержит правило 30, т.е. стандарт рекомендует выбирать выборку в 30 раз больше, чем обратная величина оцениваемых вероятностей ошибок первого и второго рода. Фактически международный стандарт [84] игнорирует эффекты блуждания и, следовательно, ошибки при его применении будут расти по мере роста объема тестовой выборки.

ЗАКЛЮЧЕНИЕ

Люди и все иные живые существа имеют сети из естественных нейронов, постоянно находящихся в режиме шумового самовозбуждения (в режиме поддержки НейроДинамики). При этом мы наблюдаем огромные интеллектуальные возможности людей, объяснить которые линейным распараллеливанием вычислений нельзя. В данной работе мы попытались показать, что перейти от простого линейного распараллеливания к экспоненциальному гиперраспараллеливанию удастся на границе перехода от анализа обычных длинных кодов в пространство кодов расстояний Хэмминга. Видимо, что-то подобное происходит в наших головах, когда мы думаем.

Если используется многократный переход границы между обычными данными и расстояниями Хэмминга, то удастся добиваться огромных ускорений при направленных переборах. При этом нет необходимости применять гипотетические квантовые логические элементы и гипотетические квантовые процессоры. То, о чем с 1980 г. говорят и пишут специалисты по квантовым вычислениям, в лице представителей физико-математической общественности, вполне возможно уже давно реализованы НейроСетями в наших головах.

Еще одним важнейшим моментом является то, что программирование квантовых высокоэффективных вычислений НейроДинамики выполняется через обучение сетей больших естественных и искусственных нейронов. В этом отношении обучение и программирование являются эквивалентами. Люди программируют себя (обучаются) самостоятельно или с учителями. Самые гениальные из нас учатся мгновенно на очень маленьких выборках. Обычные люди учатся гораздо медленнее, им приходится учиться у обычных учителей в обычных школах на обычных объемах обучающих примеров по обычным методикам обучения. То же

самое происходит и при обучении сетей искусственных нейронов. Обучение НейроСетей и программная поддержка НейроДинамики таят огромные резервы. Мы попытаюсь показать, что вполне возможно сделать уже работающий в России стандарт ГОСТ Р 52633.5 примерно в два раза гениальнее, увеличив примерно в два раза объем эквивалентной обучающей выборки.

В этом отношении современные теории квантовых вычислений, построенные на уравнениях Шредингера, имеют явный пробел. Все построенные квантовыми математиками за последние 40 лет алгоритмы направлены только на ускорение вычислений. Квантовых алгоритмов направленных на устранение неопределенности при обработке малых выборок нет. Нет попыток сокращения времени обучения и одновременного увеличения объема виртуальных примеров для обучения. Подобные алгоритмы для НейроДинамики крайне важны. Видимо, и задача ускорения вычислений, и задача повышение достоверности при обработке малых выборок должны занять свое значимое место в будущей теории НейроДинамических вычислений.

СПИСОК ЛИТЕРАТУРЫ

1. McCulloch W. S., Pitts W. A logical calculus of the ideas imminent in nervous activities // Bulletin of Mathematical Biophysics. 1943. № 5. P. 115–133.
2. URL: http://ru.wikipedia.org/Тьюринг,_Алан
3. Хайкин, С. Нейронные сети: полный курс. М. : Вильямс, 2006. С. 1104
4. ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа.
5. Малыгина Е. А. Биометрико-нейросетевая аутентификация: перспективы применения сетей квадратичных нейронов с многоуровневым квантованием биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 114 с.
6. Иванов А. И., Сулавко А. Е. Использование сетей корреляционных нейронов с многоуровневым квантованием: защита от извлечения знаний из параметров решающего правила : препринт. Пенза : Изд-во ПГУ, 2020. 48 с.
7. Иванов А. И., Куприянов Е. Н. Защита искусственного интеллекта: ортогонализация статистико-нейросетевого анализа малых выборок биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 72 с.
8. Иванов А. И., Захаров О. С. Среда моделирования «БиоНейроАвтограф». Программный продукт создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ», URL: <http://пниэи.рф/activity/science/roc/bioneuroautograph.zip>.
9. Иванов А. И. Исследование свойств нейросетевого преобразователя биометрия-код с использованием среды моделирования «БиоНейроАвтограф» : учеб.-метод. пособие. Пенза : Изд-во ПГУ, 2020. 40 с.

10. ГОСТ Р 52633.3–2011. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора.

11. 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.

12. URL: <http://ru.wikipedia.org/Энтропия>

13. Иванов А. И., Банных А. Г., Серикова Ю. И. Учет влияния корреляционных связей через их усреднение по модулю при нейросетевом обобщении статистических критериев для малых выборок // Надежность. 2020. № 20 (2). С. 28–34.

14. ГОСТ Р 52633.0–2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.

15. Волчихин В. И., Иванов А. И. Нейросетевая молекула: решение обратной задачи биометрии через программную поддержку квантовой суперпозиции на выходах сети искусственных нейронов // Вестник Мордовского университета. 2017. Т. 27, № 4. С. 518–523.

16. Иванов А. И. Искусственный интеллект высокого доверия Ускорение вычислений и экономия памяти при тестировании больших сетей искусственных нейронов на малых выборках // Системы безопасности. 2020. № 5. С. 60–62.

17. Иванов А. И., Газин А. И., Сулавко А. Е., Стадников Д. Г. Оценка ускорения вычислений в режиме программного воспроизведения эффектов нейродинамики при извлечении знаний из больших сетей искусственных нейронов // Вопросы защиты информации. 2020. № 4. С. 32–38.

18. ГОСТ Р 52633.1–2009. Защита информации. Техника защиты информации. Требования к формированию баз естественных биометри-

ческих образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации.

19. ГОСТ Р 52633.2–2010. Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации.

20. URL: http://ru.wikipedia.org/wiki/Многоядерный_процессор

21. URL: <http://ru.wikipedia.org/wiki/Нейрон>

22. Уоссермен Ф. Нейрокомпьютерная техника: теория и практика. М. : Мир, 1992. 240 с.

23. Николлс Дж. Г., Мартин Р., Валлас Б., Фукс П. От нейрона к мозгу / пер. с англ. П. М. Балабана, А. В. Галкина, Р. А. Гиниатуллина, Р. Н. Хазипова, Л. С. Хируга. М. : Едиториал УРСС, 2003. 672 с.

24. Иванов А. И., Малыгина Е. А., Лукин В. С. Компактная графическо-иероглифная система отображения схем многообразных нейросетевых вычислений // Известия высших учебных заведений. Поволжский регион. Технические науки. 2020. № 4 (56). С. 4–16.

25. Пенроуз, Р. Новый ум короля. О компьютерах, мышлении и законах физики. М. : Единориал УРСС, 2003. 339 с.

26. Гончаров С. М., Боршевников А. Е., Михайлов А. Г., Апальков А. Ю. Восстановление секретного ключа на основе электроэнцефалограмм при движении глаз с закрытыми веками // Информация и безопасность. 2016. Т. 19, № 1. С. 114–117.

27. Гончаров С. М., Боршевников А. Е. Прогнозирование выходных параметров нейросетевого преобразователя «биометрия – код доступа» на основе электроэнцефалограммы // Информация и безопасность. 2018. Т. 21, № 3. С. 302–307.

28. Боршевников А. Е., Добржинский Ю. В. О корректности модели системы высоконадежной биометрической аутентификации с исполь-

зованием электроэнцефалограммы на основе стандартов ГОСТ Р 52633 // Безопасность информационных технологий : сб. науч. ст. по материалам II Всерос. науч.-техн. конф. Пенза, 2020. С. 70–74.

29. URL: https://ru.wikipedia.org/wiki/Архитектура_фон_Неймана

30. Манин Ю. И. Вычислимое и невычислимое. М. : Сов. радио, 1980. 51 с.

31. URL: https://ru.wikipedia.org/wiki/Квантовый_компьютер

32. Гуц А. К. Основы квантовой кибернетики. М. : ЛЕНАНД, 2017. 216 с.

33. Пери Р. Элементарное введение в квантовые вычисления : учеб. пособие. М. : Интеллект, 2018. 208 с.

34. Душкин Р. В. Квантовые вычисления и функциональное программирование. М. : Пресс, 2015. 232 с.

35. URL: https://ru.wikipedia.org/wiki/Принцип_неопределенности

36. ГОСТ Р 27973.1–88. Золото. Методы атомно-эмиссионного анализа.

37. URL: https://ru.wikipedia.org/wiki/Бра_и_кет

38. Р 50.1.037–2002. Рекомендации по стандартизации. Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим. Ч. I. Критерии типа χ^2 . Госстандарт России. Москва, 2001. 140 с.

39. Р 50.1.037–2002. Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим. Ч. II. Непараметрические критерии. Госстандарт России. М., 2002. 123 с.

40. Кобзарь А. И. Прикладная математическая статистика. Для инженеров и научных работников. М. : ФИЗМАТЛИТ, 2006. 816 с.

41. Иванов А. И. Нейросетевые технологии биометрической аутентификации пользователей открытых систем : автореф. дис. на соискание ученой степени д-ра техн. наук по специальности 05.13.01 «Си-

стемный анализ, управление и обработка информации». Пенза, 2002. 34 с.

42. Иванов А. И., Банных А. Г., Серикова Ю. И. Учет влияния корреляционных связей через их усреднение по модулю при нейросетевом обобщении статистических критериев для малых выборок. Надежность. 2020. № 20 (2). С. 28–34.

43. Эйкхофф П. Основы идентификации систем управления. М. : Мир, 1975. 517 с.

44. Billings S. A. Identification of nonlinear system (A survey) // Proc. IEEE, part D. 1980. Vol. 127, № 6. P. 272–285.

45. Ли Ю., Щецен М. Определение ядер Винера-Хопфа методом взаимной корреляции // Техническая кибернетика за рубежом. М. : Машиностроение, 1968.

46. Ivanov A. I. Simple Numerical Method of Separabel Volterra Kernels Symmetrization // Engineering Simulation, 1999. № 16. P. 411–416.

47. Иванов А. И. Одномерный аналог многомерной идентификации Ли-Щецена // Управляющие системы и машины. 1999. № 2. С. 16–21.

48. Фу К. Структурные методы в распознавании образов. М. : Мир, 1977. 319 с.

49. Ту Дж., Гонсалес Р. Принципы распознавания образов. М. : Наука, 1978. 412 с.

50. Патрик Э. А. Основы теории распознавания образов. М. : Сов. радио, 1980. 407 с.

51. Иванов А. И., Перфилов К. А., Малыгина Е. А. Оценка качества малых выборок биометрических данных с использованием дифференциального варианта статистического критерия среднего геометрического // Вестник СИБГАУ. № 4 (17). 2016. С. 864–871.

52. Волчихин В. И., Иванов А. И. [и др.]. Быстрый алгоритм обучения сетей искусственных нейронов квадрата среднего геометрического плотностей распределения значений многомерных биометрических дан-

ных // Известия высших учебных заведений. Поволжский регион. Технические науки. 2018. № 3 (47). С. 23–35.

53. Иванов А. И., Перфилов К. А., Лукин В. С. Нейросетевое обобщение семейства статистических критериев среднего геометрического и среднего гармонического для прецизионного анализа малых выборок биометрических данных // Информационно-управляющие телекоммуникационные системы, средства поражения и их техническое обеспечение : сб. науч. ст. Всерос. науч.-техн. конф. / под общ. ред. В. С. Безяева. Пенза : АО «НПП “Рубин”», 2019. С. 50–63.

54. Иванов А. И., Банных А. Г. [и др.]. Коллекция искусственных нейронов эквивалентных статистическим критериям для их совместного применения при проверке гипотезы нормальности малых выборок биометрических данных // Безопасность информационных технологий : сб. науч. ст. по материалам I Всерос. науч.-техн. конф. (г. Пенза, 24 апреля). Пенза, 2019. С. 156–164.

55. Лукин В. С. Сравнение мощности обычной и логарифмической форм статистических критериев среднего гармонического при использовании для проверки гипотезы нормального распределения данных малой выборки // Известия высших учебных заведений. Поволжский регион. Технические науки. 2020. № 4. С. 19–26.

56. Лукин В. С., Калашников Д. М., Куприянов Е. Н. [и др.]. Свидетельство о госрегистрации программы для ЭВМ RU 2021661505 от 12 июля 2021 г. «Среда моделирования «БиоНейроАвтограф» с нейронами среднего гармонического». Пенза : Изд-во ПГУ, 2021.

57. Иванов А. И., Куприянов Е. Н. Защита искусственного интеллекта: ортогонализация статистико-нейросетевого анализа малых выборок биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 72 с.

58. Кулагин В., Иванов А., Газин А., Ахметов Б. Циклические континуально-квантовые вычисления: усиление мощности хи-квадрат критерия на малых выборках // Аналитика. 2016 (30). № 5. С. 88–95.

59. Волчихин В. И., Иванов А. И. [и др.]. Перспективы создания циклической континуально-квантовой хи-квадрат машины для проверки статистических гипотез на малых выборках биометрических данных и данных иной природы // Известия высших учебных заведений. Поволжский регион. Технические науки. 2017. № 1. С. 5–15.

60. Иванов А. И., Сулавко А. Е. Золотарева Т. А., Чобан А. Г. Проверка гипотезы независимости малых выборок: воспроизведение эффектов нейродинамики через случайное прореживание исходных данных // Вопросы защиты информации. 2020. № 4. С. 42–37.

61. Иванов А. И. Интеллектуализация статистической обработки малых выборок биометрических данных // Защита информации. Инсайд. 2021. № 2. С. 32–36.

62. Dahiya R. C., Gurland J. How many class in the Pearson hi-square test? // Journal of the American Statistical Association. 1973. Vol. 68, № 303. P. 707–712.

63. Ахметов Б. Б., Иванов А. И., Фунтикова Ю. В. Дискретный характер закона распределения хи-квадрат критерия для малых тестовых выборок // Вестник Национальной академии наук Республики Казахстан. 2015. № 1. С. 17–25.

64. Кулагин В. П., Ахметов Б. Б., Иванов А. И., Газин А. И. Циклические континуально-квантовые вычисления: усиление мощности хи-квадрат критерия на малых выборках // Аналитика. 2016. Т. 30, № 5. С. 22–29.

65. Иванов А. И. Искусственные математические молекулы: повышение точности статистических оценок на малых выборках (программы на языке MathCAD): препринт. Пенза : Изд-во ПГУ, 2020. 36 с.

66. Иванов А. И., Золотарева Т. А. Искусственный интеллект в защищенном исполнении: синтез статистико-нейросетевых автоматов

многокритериальной проверки гипотезы независимости малых выборок биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 105 с.

67. Волчихин В. И., Иванов А. И., Сериков А. В., Серикова Ю. И. Тестирование аналогового и квантового оракулов линейной вычислительной сложности, предсказывающих значения коэффициента корреляции на малой выборке в 32 опыта // Известия высших учебных заведений. Поволжский регион. Технические науки. 2017. № 3. С. 70–80.

68. Волчихин В. И., Иванов А. И., Сериков А. В., Серикова Ю. И. Квантовая суперпозиция дискретного спектра состояний математической молекулы корреляции для малых выборок биометрических данных // Вестник Мордовского университета. 2017. Т. 27, № 2. С. 230–243.

69. Иванов А. И. Высокоразмерная коллективная биометрия под-сознательного поведения людей на рынке и производстве : препринт. Пенза : Изд-во ПГУ, 2021. 60 с.

70. Николенко С., Кудрин А., Архангельская Е. Глубокое обучение. Погружение в мир нейронных сетей. СПб. : Питер, 2018.

71. Аггарвал Чару. Нейронные сети и глубокое обучение. СПб. : Диалектика, 2020. 756 с.

72. Волчихин В. И., Иванова Н. А., Серикова Ю. И., Банных А. Г. Синтез и тестирование оракула, способного предсказывать асимметричные границы интервала действительного положения математического ожидания малых выборок биометрических данных // Измерение. Мониторинг. Управление. Контроль. 2017. № 2 (20). С. 32–40.

73. Иванов А. И. Простейшие оракулы, обученные корректировать ошибки вычисления младших статистических моментов на малых выборках биометрических данных : учеб. пособие. Пенза : Пензенский научно-исследовательский электротехнический институт, 2018. 35 с.

74. Волчихин В. И., Иванов А. И., Серикова Ю. И. Компенсация методических погрешностей вычисления стандартных отклонений и ко-

эффицентов корреляции, возникающих из-за малого объема выборок // Известия высших учебных заведений. Поволжский регион. Технические науки. 2016. № 1. С. 45–49.

75. Волчихин В. И., Иванов А. И., Малыгина Е. А., Юнин А. П. Соотношение мощности нейронов с линейным и квадратичным обогатителями биометрических данных // Известия высших учебных заведений. Поволжский регион. Технические науки. 2018. № 1 (45). С. 17–25.

76. Волчихин В. И., Иванов А. И., Малыгина Е. А., Серикова Ю. И. Сопоставление мощности двух типов искусственных нейронов, осуществляющих обогащение биометрических данных в линейном и квадратичном пространствах // Известия высших учебных заведений. Поволжский регион. Технические науки. 2018. № 3 (47). С. 47–57.

77. Иванов А. И., Безяев А. В., Малыгина Е. А., Серикова Ю. И. Второй национальный стандарт России по быстрому автоматическому обучению больших искусственных нейронных сетей на малых выборках биометрических данных // Безопасность информационных технологий : сб. науч. ст. по материалам I Всерос. науч.-техн. конф. (г. Пенза, 24 апреля, 2019 г.). Пенза, 2019. С. 174–177.

78. Иванов А. И., Сулавко А. Е. Использование сетей корреляционных нейронов с многоуровневым квантованием: защита от извлечения знаний из параметров решающего правила : препринт. Пенза : Изд-во ПГУ, 2020. 48 с.

79. Иванов А. И., Сулавко А. Е. Проект третьего национального стандарта России по быстрому автоматическому обучению больших сетей корреляционных нейронов на малых обучающих выборках биометрических данных // Вопросы кибербезопасности. 2021. № 3 (43). С. 84–93.

80. Волчихин В. И., Иванов А. И., Сериков А. В., Серикова Ю. И. Квантовая суперпозиция дискретного спектра состояний математической

молекулы корреляции для малых выборок биометрических данных // Вестник Мордовского университета. 2017. Т. 27, № 2. С. 230–243.

81. Иванов А. И., Сулавко А. Е., Золотарева Т. А., Чобан А. Г. Проверка гипотезы независимости малых выборок: воспроизведение эффектов нейродинамики через случайное прореживание исходных данных // Вопросы защиты информации, 2020. № 4. С. 37–42.

82. Ivanov, A. I., Gazin, A. I., Zolotareva, T. A. Use of Bootstrap Interface for Implementation of the Algorithm of a Small Sample Increase of Biometric Data // Lecture Notes in Electrical Engineering. 2021. 729 LNEE. С. 513–522.

83. Золотарева Т. А. Аналоги корреляционного критерия Пирсона // Информатика и вычислительная техника и управление. Сер.: Естественные и технические науки. 2021. № 4. С. 90–97.

84. ГОСТ Р ИСО/МЭК 19795-1–2007. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Ч. 1. Принципы и структура.

Приложение 1

Численное моделирование шести статистических критериев для проверки гипотезы нормального распределения выборок, объемом по 16 опытов (KfM – Крамера – фон Мизеса; χ^2 ; SKfM – Смирнова – Крамера – фон Мизеса; AD – Андерсона – Дарлингга; F – Фроцини; MT – Муроты – Такеучи; V – Васичека)

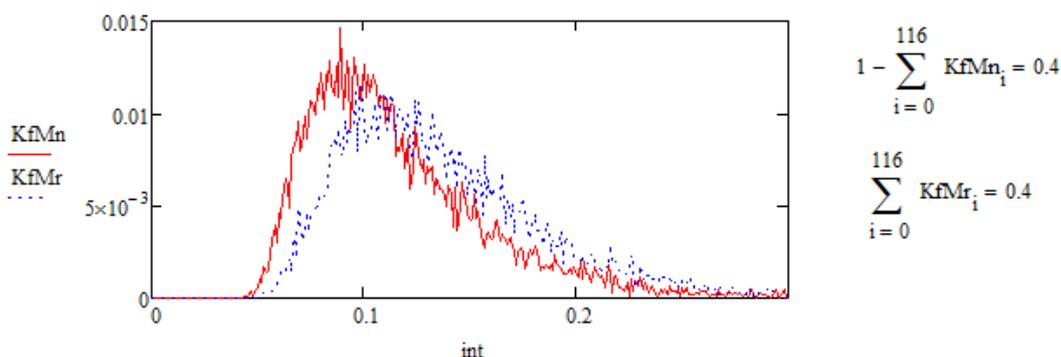
$ \begin{aligned} \text{sx}(\text{rr}) := & \quad x \leftarrow \text{sort}(\text{morm}(16, 0, 1 + \text{rr})) \\ & \quad m \leftarrow \text{mean}(x) \\ & \quad \sigma \leftarrow \text{stdev}(x) \\ \text{KfM} \leftarrow & \quad \sum_{i=0}^{15} \left(\text{pnorm}(x_i, m, \sigma) - \frac{i - 0.5}{16} \right)^2 \\ \text{SKfM} \leftarrow & \quad \sum_{i=0}^{15} \left[\left(\text{pnorm}(x_i, m, \sigma) - \frac{i - 0.5}{16} \right)^2 \cdot \text{dnorm}(x_i, m, \sigma) \right] \\ \text{for } i \in & \quad 0..6 \\ & \quad \left \begin{aligned} \text{int}_i \leftarrow & \quad \frac{(x_{15} - x_0) \cdot i}{6} + x_0 \\ \text{P}_i \leftarrow & \quad \text{pnorm} \left[\frac{(x_{15} - x_0) \cdot i}{6} + x_0, m, \sigma \right] \end{aligned} \right. \\ n \leftarrow & \quad \text{hist}(\text{int}, x) \\ \chi^2 \leftarrow & \quad \sum_{i=0}^5 \frac{[n_i - 16 \cdot (P_{i+1} - P_i)]^2}{16 \cdot (P_{i+1} - P_i)} \\ \text{AD} \leftarrow & \quad \sum_{i=0}^{15} \frac{\left(\text{pnorm}(x_i, m, \sigma) - \frac{i - 0.5}{16} \right)^2 \cdot \text{dnorm}(x_i, m, \sigma)}{\text{pnorm}(x_i, m, \sigma) \cdot (1 - \text{pnorm}(x_i, m, \sigma))} \\ \text{F} \leftarrow & \quad \sum_{i=0}^{15} \left[\left \text{pnorm}(x_i, m, \sigma) - \frac{i - 0.5}{16} \right \cdot \text{dnorm}(x_i, m, \sigma) \right] \\ \text{MT} \leftarrow & \quad \sum_{i=0}^{15} \left(\cos \left(\frac{x_i - x_{15}}{1.8} \right) \right) \\ \text{V4} \leftarrow & \quad \left[\prod_{i=0}^{10} (x_{i+4} - x_i) \right]^{\frac{1}{11}} \\ & \quad (\text{KfM } \chi^2 \text{ SKfM } \text{AD } \text{F } \text{MT } \text{V4})^T \end{aligned} $	$ \begin{aligned} \text{sxr}(\text{rr}) := & \quad x \leftarrow \text{sort}(\text{runif}(16, -3 - \text{rr}, 3 + \text{rr})) \\ & \quad m \leftarrow \text{mean}(x) \\ & \quad \sigma \leftarrow \text{stdev}(x) \\ \text{KfM} \leftarrow & \quad \sum_{i=0}^{15} \left(\text{pnorm}(x_i, m, \sigma) - \frac{i - 0.5}{16} \right)^2 \\ \text{SKfM} \leftarrow & \quad \sum_{i=0}^{15} \left[\left(\text{pnorm}(x_i, m, \sigma) - \frac{i - 0.5}{16} \right)^2 \cdot \text{dnorm}(x_i, m, \sigma) \right] \\ \text{for } i \in & \quad 0..6 \\ & \quad \left \begin{aligned} \text{int}_i \leftarrow & \quad \frac{(x_{15} - x_0) \cdot i}{6} + x_0 \\ \text{P}_i \leftarrow & \quad \text{pnorm} \left[\frac{(x_{15} - x_0) \cdot i}{6} + x_0, m, \sigma \right] \end{aligned} \right. \\ n \leftarrow & \quad \text{hist}(\text{int}, x) \\ \chi^2 \leftarrow & \quad \sum_{i=0}^5 \frac{[n_i - 16 \cdot (P_{i+1} - P_i)]^2}{16 \cdot (P_{i+1} - P_i)} \\ \text{AD} \leftarrow & \quad \sum_{i=0}^{15} \frac{\left(\text{pnorm}(x_i, m, \sigma) - \frac{i - 0.5}{16} \right)^2 \cdot \text{dnorm}(x_i, m, \sigma)}{\text{pnorm}(x_i, m, \sigma) \cdot (1 - \text{pnorm}(x_i, m, \sigma))} \\ \text{F} \leftarrow & \quad \sum_{i=0}^{15} \left[\left \text{pnorm}(x_i, m, \sigma) - \frac{i - 0.5}{16} \right \cdot \text{dnorm}(x_i, m, \sigma) \right] \\ \text{MT} \leftarrow & \quad \sum_{i=0}^{15} \left(\cos \left(\frac{x_i - x_{15}}{1.8} \right) \right) \\ \text{V4} \leftarrow & \quad \left[\prod_{i=0}^{10} (x_{i+4} - x_i) \right]^{\frac{1}{11}} \\ & \quad (\text{KfM } \chi^2 \text{ SKfM } \text{AD } \text{F } \text{MT } \text{V4})^T \end{aligned} $
---	--

$$\begin{aligned}
 i := & \quad 0..9999 \quad \text{rr}_i := \text{md}(0.01) \quad X^{(i)} := \text{sx}(\text{rr}_i) \quad C := X^T \quad Xr^{(i)} := \text{sxr}(\text{rr}_i) \quad Cr := Xr^T \\
 \text{xx0} := & \quad C^{(0)} \quad \text{xxr0} := Cr^{(0)} \quad \text{xx1} := C^{(1)} \quad \text{xxr1} := Cr^{(1)} \quad \text{xx2} := C^{(2)} \quad \text{xxr2} := Cr^{(2)} \quad \text{xx6} := C^{(6)} \\
 \text{xx3} := & \quad C^{(3)} \quad \text{xxr3} := Cr^{(3)} \quad \text{xx4} := C^{(4)} \quad \text{xxr4} := Cr^{(4)} \quad \text{xx5} := C^{(5)} \quad \text{xxr5} := Cr^{(5)} \quad \text{xxr6} := Cr^{(6)}
 \end{aligned}$$

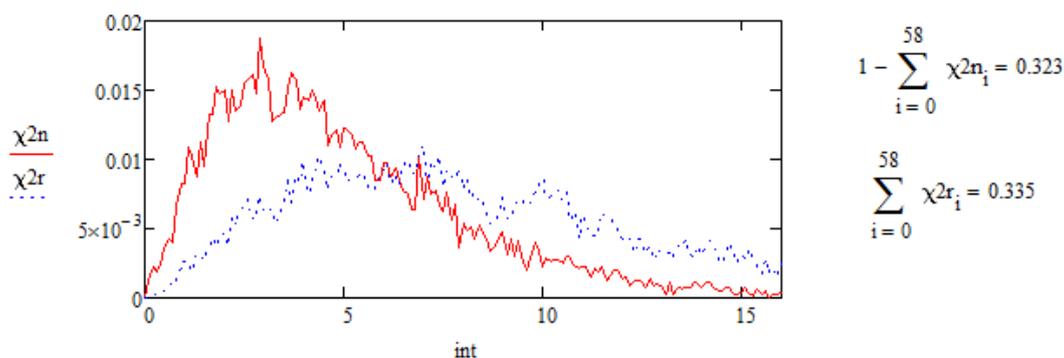
Продолжение приложения 1

Графики распределение данных трех статистических критериев: KfM – Крамера – фон Мизеса; χ^2 ; SKfM – Смирнова – Крамера – фон Мизеса

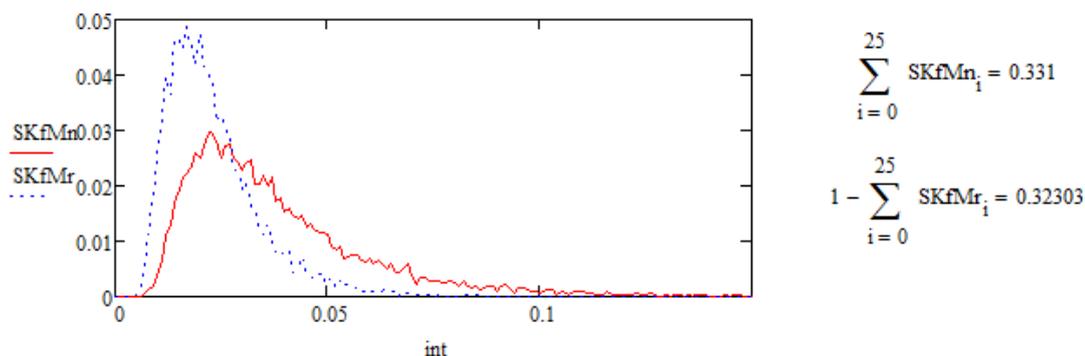
$$j := 0..999 \quad \text{int}_j := 0 + 0.001 \cdot j \quad \text{KfMn} := \frac{\text{hist}(\text{int}, \text{xx0})}{9999} \quad \text{KfMr} := \frac{\text{hist}(\text{int}, \text{xxr0})}{9999}$$



$$j := 0..999 \quad \text{int}_j := 0 + 0.1 \cdot j \quad \chi^2n := \frac{\text{hist}(\text{int}, \text{xx1})}{9999} \quad \chi^2r := \frac{\text{hist}(\text{int}, \text{xxr1})}{9999}$$

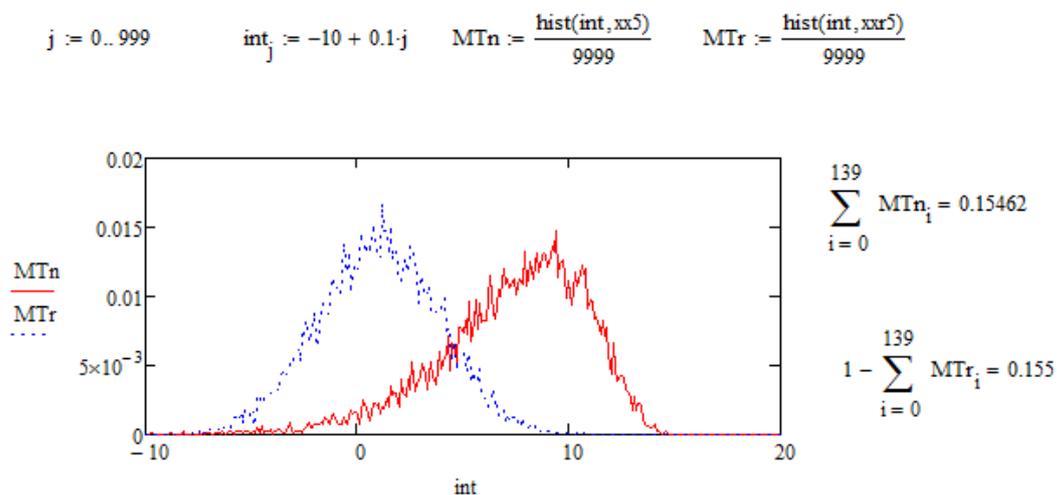
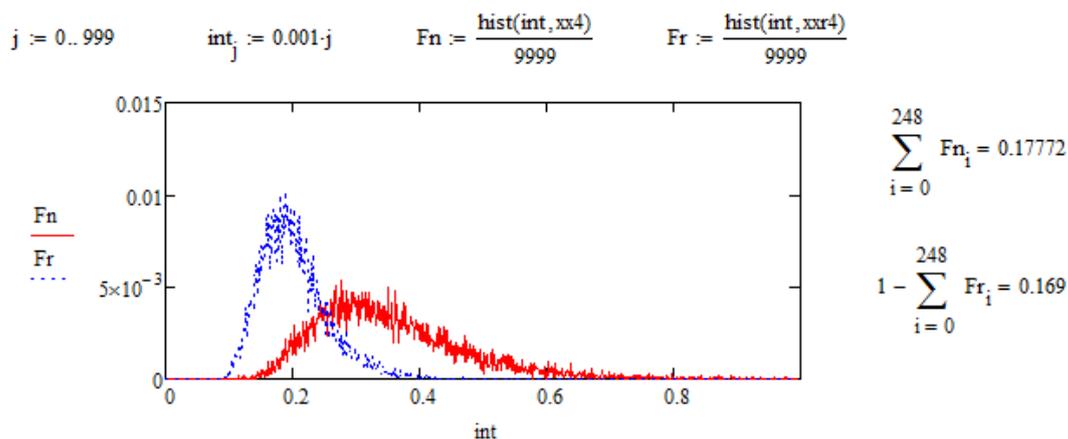
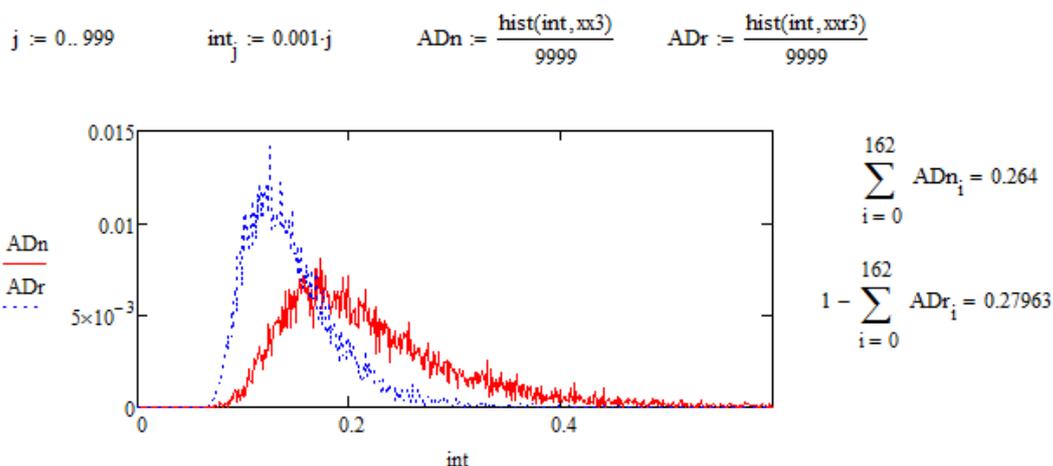


$$j := 0..999 \quad \text{int}_j := 0.001 \cdot j \quad \text{SKfMn} := \frac{\text{hist}(\text{int}, \text{xx2})}{9999} \quad \text{SKfMr} := \frac{\text{hist}(\text{int}, \text{xxr2})}{9999}$$



Продолжение приложения 1

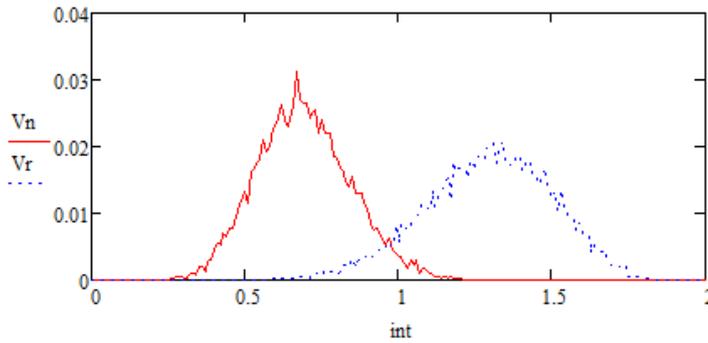
Графики распределение данных трех статистических критериев: *AD* - Андерсона - Дарлингга; *F* - Фроцини; *MT* - Муроты - Такеучи



Продолжение приложения 1

Распределение значений критерия Васичека и вычисление корреляционной матрицы со средним значением модулей корреляции

$$j := 0..999 \quad \text{int}_j := 0 + 0.01 \cdot j \quad V_n := \frac{\text{hist}(\text{int}, \text{xx6})}{9999} \quad V_r := \frac{\text{hist}(\text{int}, \text{xxr6})}{9999}$$



$$1 - \sum_{i=0}^{93} V_{n_i} = 0.061$$

$$\sum_{i=0}^{93} V_{r_i} = 0.05021$$

$$\sqrt[7]{0.405 - 0.33 - 0.32 - 0.27 - 0.17 - 0.155 - 0.055} = 0.208$$

$$\begin{aligned} r_{01} &:= \text{corr}(C^{(0)}, C^{(1)}) & r_{03} &:= \text{corr}(C^{(0)}, C^{(3)}) & r_{05} &:= \text{corr}(C^{(0)}, C^{(5)}) & r_{01} &= 0.496 & r_{03} &= 0.848 \\ r_{02} &:= \text{corr}(C^{(0)}, C^{(2)}) & r_{04} &:= \text{corr}(C^{(0)}, C^{(4)}) & r_{06} &:= \text{corr}(C^{(0)}, C^{(6)}) & r_{02} &= 0.899 & r_{04} &= 0.727 \\ & & & & & & r_{05} &= 0.378 & r_{06} &= -0.136 \end{aligned}$$

$$\text{mr0} := \text{mean}(0.496, 0.899, 0.848, 0.727, 0.378, 0.136) \quad \text{mr0} = 0.581$$

$$\begin{aligned} r_{12} &:= \text{corr}(C^{(1)}, C^{(2)}) & r_{13} &:= \text{corr}(C^{(1)}, C^{(3)}) & r_{14} &:= \text{corr}(C^{(1)}, C^{(4)}) & r_{12} &= 0.359 & r_{13} &= 0.459 \\ r_{15} &:= \text{corr}(C^{(1)}, C^{(5)}) & r_{16} &:= \text{corr}(C^{(1)}, C^{(6)}) & r_{14} &= 0.246 & r_{15} &= 0.123 & r_{16} &= -0.083 \end{aligned}$$

$$\text{mr1} := \text{mean}(0.359, 0.459, 0.246, 0.123, 0.083) \quad \text{mr1} = 0.254$$

$$\begin{aligned} r_{23} &:= \text{corr}(C^{(2)}, C^{(3)}) & r_{24} &:= \text{corr}(C^{(2)}, C^{(4)}) & r_{25} &:= \text{corr}(C^{(2)}, C^{(5)}) \\ r_{25} &:= \text{corr}(C^{(2)}, C^{(5)}) & r_{26} &:= \text{corr}(C^{(2)}, C^{(6)}) & r_{23} &= 0.951 & r_{24} &= 0.931 & r_{25} &= 0.555 & r_{26} &= -0.406 \end{aligned}$$

$$\text{mr2} := \text{mean}(0.951, 0.931, 0.555, 0.406) \quad \text{mr2} = 0.711$$

$$\begin{aligned} r_{34} &:= \text{corr}(C^{(3)}, C^{(4)}) & r_{34} &:= \text{corr}(C^{(3)}, C^{(4)}) & r_{35} &:= \text{corr}(C^{(3)}, C^{(5)}) & r_{34} &= 0.917 & r_{35} &= 0.63 \\ r_{36} &:= \text{corr}(C^{(3)}, C^{(6)}) & r_{45} &:= \text{corr}(C^{(4)}, C^{(5)}) & r_{46} &:= \text{corr}(C^{(4)}, C^{(6)}) & r_{36} &= -0.526 & r_{45} &= 0.674 \\ & & & & & & r_{46} &= -0.579 \end{aligned}$$

$$\text{mr3} := \text{mean}(0.917, 0.63, 0.526, 0.674, 0.579) \quad \text{mr3} = 0.665$$

$$\text{mean}(\text{mr0}, \text{mr1}, \text{mr2}, \text{mr3}) = 0.553$$

Моделирование кодовых откликов в пространстве расстояний Хэмминга симметричных сетей искусственных нейронов с 16 выходами

$$\begin{aligned}
 a &:= 0.92 & n &:= 99999 & z &:= \text{mom}(n, 0, 1) & x^{(0)} &:= \text{mom}(n, 0, 1) & x^{(1)} &:= \text{mom}(n, 0, 1) & x^{(2)} &:= \text{mom}(n, 0, 1) \\
 x^{(3)} &:= \text{mom}(n, 0, 1) & x^{(4)} &:= \text{mom}(n, 0, 1) & x^{(5)} &:= \text{mom}(n, 0, 1) & x^{(6)} &:= \text{mom}(n, 0, 1) & x^{(7)} &:= \text{mom}(n, 0, 1) \\
 x^{(8)} &:= \text{mom}(n, 0, 1) & x^{(9)} &:= \text{mom}(n, 0, 1) & x^{(10)} &:= \text{mom}(n, 0, 1) & x^{(11)} &:= \text{mom}(n, 0, 1) & x^{(12)} &:= \text{mom}(n, 0, 1) \\
 x^{(13)} &:= \text{mom}(n, 0, 1) & x^{(14)} &:= \text{mom}(n, 0, 1) & x^{(15)} &:= \text{mom}(n, 0, 1) & x^{(15)} &:= \frac{a \cdot x^{(15)} + z}{\sqrt{1 + a^2}}
 \end{aligned}$$

$$x^{(0)} := \frac{a \cdot x^{(0)} + z}{\sqrt{1 + a^2}} \quad x^{(1)} := \frac{a \cdot x^{(1)} + z}{\sqrt{1 + a^2}} \quad x^{(2)} := \frac{a \cdot x^{(2)} + z}{\sqrt{1 + a^2}} \quad x^{(3)} := \frac{a \cdot x^{(3)} + z}{\sqrt{1 + a^2}} \quad x^{(4)} := \frac{a \cdot x^{(4)} + z}{\sqrt{1 + a^2}}$$

$$x^{(5)} := \frac{a \cdot x^{(5)} + z}{\sqrt{1 + a^2}} \quad x^{(6)} := \frac{a \cdot x^{(6)} + z}{\sqrt{1 + a^2}} \quad x^{(7)} := \frac{a \cdot x^{(7)} + z}{\sqrt{1 + a^2}} \quad x^{(8)} := \frac{a \cdot x^{(8)} + z}{\sqrt{1 + a^2}} \quad x^{(9)} := \frac{a \cdot x^{(9)} + z}{\sqrt{1 + a^2}}$$

$$x^{(10)} := \frac{a \cdot x^{(10)} + z}{\sqrt{1 + a^2}} \quad x^{(11)} := \frac{a \cdot x^{(11)} + z}{\sqrt{1 + a^2}} \quad x^{(12)} := \frac{a \cdot x^{(12)} + z}{\sqrt{1 + a^2}} \quad x^{(13)} := \frac{a \cdot x^{(13)} + z}{\sqrt{1 + a^2}} \quad x^{(14)} := \frac{a \cdot x^{(14)} + z}{\sqrt{1 + a^2}}$$

$$\begin{aligned}
 \text{corr}(x^{(0)}, x^{(1)}) &= 0.542 & \text{corr}(x^{(0)}, x^{(2)}) &= 0.545 & \text{corr}(x^{(1)}, x^{(2)}) &= 0.542 & \text{corr}(x^{(1)}, x^{(3)}) &= 0.54 & \text{corr}(x^{(1)}, x^{(6)}) &= 0.541 \\
 \text{corr}(x^{(1)}, x^{(4)}) &= 0.542 & \text{corr}(x^{(2)}, x^{(4)}) &= 0.54 & \text{corr}(x^{(0)}, x^{(4)}) &= 0.54 & \text{corr}(x^{(0)}, x^{(5)}) &= 0.544 & \text{corr}(x^{(0)}, x^{(6)}) &= 0.543
 \end{aligned}$$

$$\begin{aligned}
 p &:= -0.81 & p0 &:= \begin{cases} k \leftarrow 0 \\ \text{for } i \in 0..99998 \\ k \leftarrow k + 1 \text{ if } (x^{(0)})_i < p \\ k - 0.00001 \end{cases} & p0 &= 0.21 & p & & a & & r \\
 & & & & & & -0.81 & & 0.9 & & 0.55
 \end{aligned}$$

$$\begin{aligned}
 w0 &:= \begin{cases} \text{for } i \in 0..99998 \\ w0_i \leftarrow 0 \\ w0_i \leftarrow 1 \text{ if } (x^{(0)})_i < p \\ w0 \end{cases} & w1 &:= \begin{cases} \text{for } i \in 0..99998 \\ w1_i \leftarrow 0 \\ w1_i \leftarrow 1 \text{ if } (x^{(1)})_i < p \\ w1 \end{cases} & w2 &:= \begin{cases} \text{for } i \in 0..99998 \\ w2_i \leftarrow 0 \\ w2_i \leftarrow 1 \text{ if } (x^{(2)})_i < p \\ w2 \end{cases}
 \end{aligned}$$

$$h3 := w0 + w1 + w2$$

$$\begin{aligned}
 j &:= 0..9999 & \text{int}_j &:= 0 + 0.01 \cdot j & \text{hh3} &:= \frac{\text{hist}(\text{int}, h3)}{99998} \\
 \text{hh3}_0 &= 0.607 & \text{hh3}_{100} &= 0.219 & \text{hh3}_{200} &= 0.113972 & \text{hh3}_{300} &= 0.060271 \\
 1 - \text{hh3}_0 - \text{hh3}_{100} &= 0.17423
 \end{aligned}$$



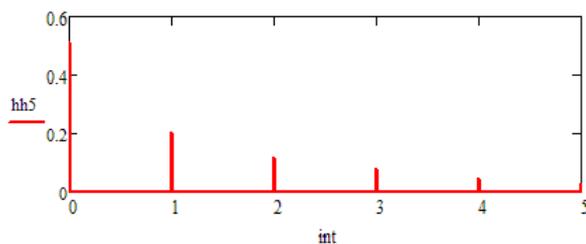
Продолжение приложения 2

Получение графика снижения вероятностей ошибок при двойном логарифмировании осей

$$\begin{array}{l}
 w3 := \left[\begin{array}{l} \text{for } i \in 0..99998 \\ \quad w3_i \leftarrow 0 \\ \quad w3_i \leftarrow 1 \text{ if } (x^{(3)})_i < p \\ \quad w3 \end{array} \right. \\
 w4 := \left[\begin{array}{l} \text{for } i \in 0..99998 \\ \quad w4_i \leftarrow 0 \\ \quad w4_i \leftarrow 1 \text{ if } (x^{(4)})_i < p \\ \quad w4 \end{array} \right. \\
 h5 := w0 + w1 + w2 + w3 + w4 \\
 hh5 := \frac{\text{hist}(\text{int}, h5)}{99998}
 \end{array}$$

$$hh5_0 = 0.513 \quad hh5_{100} = 0.205 \quad hh5_{200} = 0.120472 \quad hh5_{300} = 0.079002 \quad hh5_{400} = 0.051351$$

$$1 - hh5_0 - hh5_{100} - hh5_{200} = 0.16187$$



$$\begin{array}{l}
 w5 := \left[\begin{array}{l} \text{for } i \in 0..99998 \\ \quad w5_i \leftarrow 0 \\ \quad w5_i \leftarrow 1 \text{ if } (x^{(5)})_i < p \\ \quad w5 \end{array} \right. \\
 w6 := \left[\begin{array}{l} \text{for } i \in 0..99998 \\ \quad w6_i \leftarrow 0 \\ \quad w6_i \leftarrow 1 \text{ if } (x^{(6)})_i < p \\ \quad w6 \end{array} \right.
 \end{array}$$

$$h7 := w0 + w1 + w2 + w3 + w4 + w5 + w6 \quad hh7 := \frac{\text{hist}(\text{int}, h7)}{99998}$$

$$hh7_0 = 0.453$$

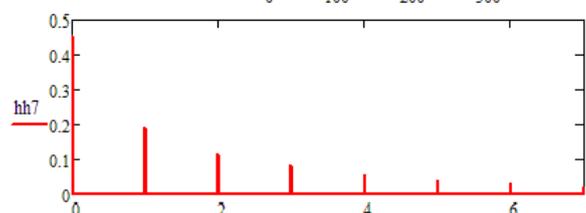
$$hh7_{100} = 0.191$$

$$hh7_{200} = 0.118$$

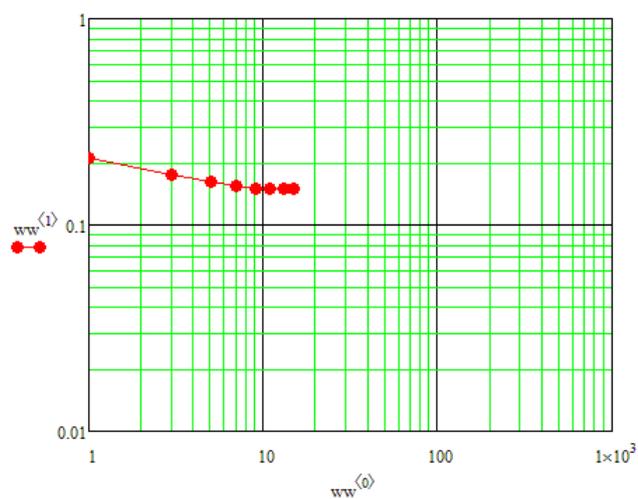
$$hh7_{300} = 0.083$$

$$hh7_{400} = 0.06$$

$$1 - hh7_0 - hh7_{100} - hh7_{200} - hh7_{300} = 0.15533$$



$$ww := \left(\begin{array}{l} 1 \quad 0.21 \\ 3 \quad 0.175 \\ 5 \quad 0.163 \\ 7 \quad 0.155 \\ 9 \quad 0.151 \\ 11 \quad 0.150 \\ 13 \quad 0.149 \\ 15 \quad 0.149 \end{array} \right)$$



Приложение 3

Формирование колоды из 64 карт случайным отбрасыванием по 5 опытов из первоначальной избыточной выборки в 21 опыт

```

w := for i ∈ 0..20
      wi ← i
      for i ∈ 0..999
        A ← w0
        a ← floor(md(20.49))
        B ← wa
        wa ← A
        w0 ← B
        i := 0..15
        s16i := s21i
w
    
```

$$s16^T =$$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	9	11	7	6	20	15	14	10	1	13	5	0	18	12	16	3

WRITEPRN("s16T.pm") := ■ APPENDPRN("s16T.pm") := s16^T ss16T := READPRN("s16T.pm")

$$ss16^T =$$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	8	17	7	9	19	3	6	16	0	15	4	2	11	5	20
1	11	8	14	3	15	19	17	13	16	7	9	6	2	4	10	1
2	10	2	15	19	3	0	16	17	18	14	6	20	7	12	9	5
3	6	12	1	19	11	16	7	8	3	18	4	15	17	0	13	14
4	20	12	8	1	16	19	7	3	15	2	13	14	4	10	17	18
5	16	2	17	3	1	12	11	0	9	6	14	10	20	18	19	13
6	3	7	1	15	20	14	4	17	6	19	0	13	12	8	5	11
7	8	17	15	18	20	3	7	4	13	5	1	10	12	14	16	9
8	4	18	17	10	16	8	11	15	1	12	2	5	19	9	20	7
9	6	16	20	5	12	15	13	17	18	7	1	3	19	14	8	9
10	9	17	7	20	1	6	11	3	15	4	12	14	16	10	13	5
11	6	5	15	1	19	20	18	3	2	10	7	16	12	9	8	4
12	8	20	10	16	6	9	13	14	1	15	12	2	0	7	18	19
13	6	19	10	18	8	13	14	15	16	9	12	1	4	5	0	17
14	6	13	10	20	5	7	19	18	0	14	9	12	1	15	11	17
15	9	20	17	12	16	4	11	14	8	6	0	10	3	2	18	...

$$\text{last}(ss16^T \binom{0}{}) = 64$$

Продолжение приложения 3

Вычисление расстояний Хэмминга одной малой выборки в 21 опыт после модулирования данных НейроСети из 5 НейроКритериев (SKfM, AD, F, MT, V) случайным прореживанием

```

x := mom(21,0,1)
ss16T := READPRN("s16T.pm")  n := ss16TT
r := runif(21,-3,3)

sx(x) :=
x ← sort(x)
m ← mean(x)
σ ← stdev(x)
SKfM ← ∑i=015 [ (pnom(xi,m,σ) -  $\frac{i-0.5}{16}$ )2 · dnom(xi,m,σ) ]
AD ← ∑i=015 [  $\frac{(\text{pnom}(x_i,m,\sigma) - \frac{i-0.5}{16}) \cdot \text{dnom}(x_i,m,\sigma)}{\text{pnom}(x_i,m,\sigma) \cdot (1 - \text{pnom}(x_i,m,\sigma))}$  ]
F ← ∑i=015 [ | (pnom(xi,m,σ) -  $\frac{i-0.5}{16}$ ) | · dnom(xi,m,σ) ]
MT ← ∑i=015 ( cos( $\frac{x_i - x_{15}}{1.8}$ ) )
V4 ← [ ∏i=010 (xi+4 - xi) ] $\frac{1}{11}$ 
k ← (1 1 1 1 1)T
k0 ← 0 if SKfM > 0.025
k1 ← 0 if AD > 0.162
k2 ← 0 if F > 0.248
k3 ← 0 if MT > 3.9
k4 ← 0 if V4 < 0.93
h ← k4 + k3 + k2 + k1 + k0
h

sxr(r) :=
r ← sort(r)
m ← mean(r)
σ ← stdev(r)
SKfM ← ∑i=015 [ (pnom(ri,m,σ) -  $\frac{i-0.5}{16}$ )2 · dnom(ri,m,σ) ]
AD ← ∑i=015 [  $\frac{(\text{pnom}(r_i,m,\sigma) - \frac{i-0.5}{16}) \cdot \text{dnom}(r_i,m,\sigma)}{\text{pnom}(r_i,m,\sigma) \cdot (1 - \text{pnom}(r_i,m,\sigma))}$  ]
F ← ∑i=015 [ | (pnom(ri,m,σ) -  $\frac{i-0.5}{16}$ ) | · dnom(ri,m,σ) ]
MT ← ∑i=015 ( cos( $\frac{r_i - r_{15}}{1.8}$ ) )
V4 ← [ ∏i=010 (ri+4 - ri) ] $\frac{1}{11}$ 
k ← (1 1 1 1 1)T
k0 ← 0 if SKfM > 0.025
k1 ← 0 if AD > 0.162
k2 ← 0 if F > 0.248
k3 ← 0 if MT > 3.9
k4 ← 0 if V4 < 0.93
h ← k4 + k3 + k2 + k1 + k0
h

i := 0..64

```

$$x16^{(i)} = [x_{[n^{(i)}_0]}^{(i)}, x_{[n^{(i)}_1]}^{(i)}, x_{[n^{(i)}_2]}^{(i)}, x_{[n^{(i)}_3]}^{(i)}, x_{[n^{(i)}_4]}^{(i)}, x_{[n^{(i)}_5]}^{(i)}, x_{[n^{(i)}_6]}^{(i)}, x_{[n^{(i)}_7]}^{(i)}, x_{[n^{(i)}_8]}^{(i)}, x_{[n^{(i)}_9]}^{(i)}, x_{[n^{(i)}_{10}]}^{(i)}, x_{[n^{(i)}_{11}]}^{(i)}, x_{[n^{(i)}_{12}]}^{(i)}, x_{[n^{(i)}_{13}]}^{(i)}, x_{[n^{(i)}_{14}]}^{(i)}, x_{[n^{(i)}_{15}]}^{(i)}]^T$$

$$r16^{(i)} = [r_{[n^{(i)}_0]}^{(i)}, r_{[n^{(i)}_1]}^{(i)}, r_{[n^{(i)}_2]}^{(i)}, r_{[n^{(i)}_3]}^{(i)}, r_{[n^{(i)}_4]}^{(i)}, r_{[n^{(i)}_5]}^{(i)}, r_{[n^{(i)}_6]}^{(i)}, r_{[n^{(i)}_7]}^{(i)}, r_{[n^{(i)}_8]}^{(i)}, r_{[n^{(i)}_9]}^{(i)}, r_{[n^{(i)}_{10}]}^{(i)}, r_{[n^{(i)}_{11}]}^{(i)}, r_{[n^{(i)}_{12}]}^{(i)}, r_{[n^{(i)}_{13}]}^{(i)}, r_{[n^{(i)}_{14}]}^{(i)}, r_{[n^{(i)}_{15}]}^{(i)}]^T$$

$$a_i := \text{sx}[x16^{(i)}] \quad \text{mean}(a) = 0.569 \quad ar_i := \text{sxr}[r16^{(i)}] \quad \text{mean}(ar) = 4.969$$

$$a^T =$$

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
0	0	3	0	0	0	0	0	0	0	0	0	1	0	0	0	2	3	0	0	2	0	0	3	...

$$ar^T =$$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	...

Численное моделирование дискретной хи-квadrat молекулы Пирсона для малых выборок из 16 опытов с нормальным и равномерным распределением

```

sx(rr) :=
  x ← sort(mnorm(16,0,1 + rr))
  m ← mean(x)
  σ ← stdev(x)
  for i ∈ 0..6
    inti ← (i - 3)·σ + m
    Pi ← pnorm([(i - 3)·σ + m],m,σ)
  n ← hist(int,x)
  χ2 ← ∑i=05  $\frac{[n_i - 16 \cdot (P_{i+1} - P_i)]^2}{16 \cdot (P_{i+1} - P_i)}$ 
  χ2

```

```

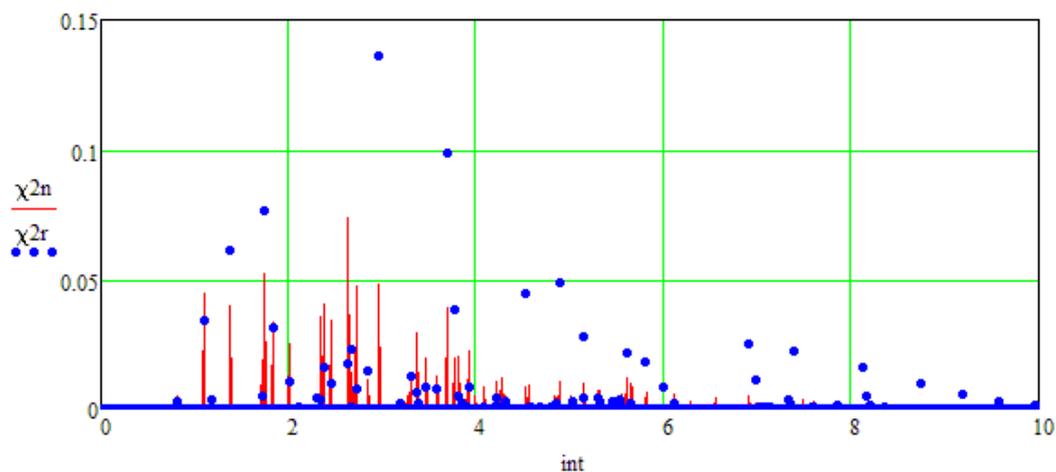
sxr(rr) :=
  x ← sort(runif(16,-3 - rr,3 + rr))
  m ← mean(x)
  σ ← stdev(x)
  for i ∈ 0..6
    inti ← (i - 3)·σ + m
    Pi ← pnorm([(i - 3)·σ + m],m,σ)
  n ← hist(int,x)
  χ2 ← ∑i=05  $\frac{[n_i - 16 \cdot (P_{i+1} - P_i)]^2}{16 \cdot (P_{i+1} - P_i)}$ 
  χ2

```

i := 0..9999

rr_i := md(0.01) xx0_i := (sx(rr_i)) xxr0_i := (sxr(rr_i))

j := 0..999 int_j := 0.01·j χ²_{2n} := $\frac{\text{hist}(\text{int}, \text{xx0})}{9999}$ χ²_{2r} := $\frac{\text{hist}(\text{int}, \text{xxr0})}{9999}$



Продолжение приложения 4

**Оценка амплитуд вероятности порядка
200 значимых спектральных линий хи-квадрат
молекулы, возбуждаемых малыми выборками
в 16 опытов с нормальным
и равномерным распределением значений**

```

a := sort(xr0)      b := sort(xsr0)
i := 0..9998      aq := round(ai,2)    bq := round(bi,2)
dxni := ai+1 - ai    dxri := bi+1 - bi

pLn := | n ← 0
      | for i ∈ 0..9998
      |   n ← n + 1 if dxni > 0.01
      |   fn ← ai if dxni > 0.01
      |   In ← i if dxni > 0.01
      |   ww(0) ← f
      |   ww(1) ← I
      |   for i ∈ 1..last(ww(0))
      |     hi ← Ii - Ii-1
      |   ww(2) ← h
      |   ww

pLr := | n ← 0
      | for i ∈ 0..9998
      |   n ← n + 1 if dxri > 0.01
      |   fn ← bi if dxri > 0.01
      |   In ← i if dxri > 0.01
      |   ww(0) ← f
      |   ww(1) ← I
      |   for i ∈ 1..last(ww(0))
      |     hi ← Ii - Ii-1
      |   ww(2) ← h
      |   ww
    
```

	0
42	0
43	0
44	0
45	0
46	0
47	0
48	0
49	0
50	0
51	0
52	0
53	0.28
54	0
55	0
56	0
57	0
58	0
59	0
60	...

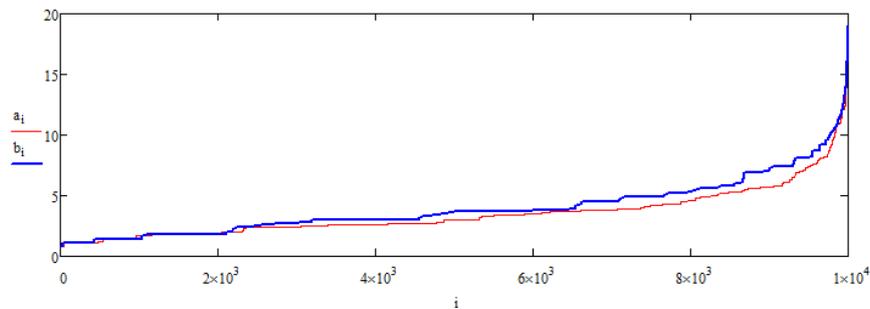
	0
42	0.82
43	0.82
44	0.82
45	0.82
46	0.82
47	0.82
48	0.82
49	0.82
50	0.82
51	0.82
52	0.82
53	0.82
54	1.1
55	1.1
56	1.1
57	1.1
58	1.1
59	1.1
60	...

	0	1	2
0	0	0	0
1	0.82	53	53
2	1.1	477	424
3	1.19	537	60
4	1.39	952	415
5	1.44	953	1
6	1.72	954	1
7	1.73	1160	206
8	1.74	1163	3
9	1.76	1680	517
10	1.81	1685	5
11	1.82	1686	1
12	1.84	2052	366
13	2.01	2304	252
14	2.1	2318	14
15	2.28	2324	6
16	2.31	2352	28
17	2.36	2674	322
18	2.38	3059	385
19	2.46	3387	...

	0	1	2
0	0	0	0
1	0.82	33	33
2	1.1	415	382
3	1.19	435	20
4	1.39	1037	602
5	1.73	1083	46
6	1.74	1084	1
7	1.76	1808	724
8	1.84	2106	298
9	2.01	2183	77
10	2.1	2193	10
11	2.28	2196	3
12	2.31	2236	40
13	2.36	2283	47
14	2.38	2452	169
15	2.46	2546	94
16	2.55	2548	2
17	2.63	2549	1
18	2.65	2706	157
19	2.66	2720	...

	0
25	0
26	0
27	0
28	0
29	0
30	0
31	0
32	0
33	0.28
34	0
35	0
36	0
37	0
38	0
39	0
40	0
41	0
42	...

	0
25	0.82
26	0.82
27	0.82
28	0.82
29	0.82
30	0.82
31	0.82
32	0.82
33	0.82
34	1.1
35	1.1
36	1.1
37	1.1
38	1.1
39	1.1
40	1.1
41	1.1
42	...

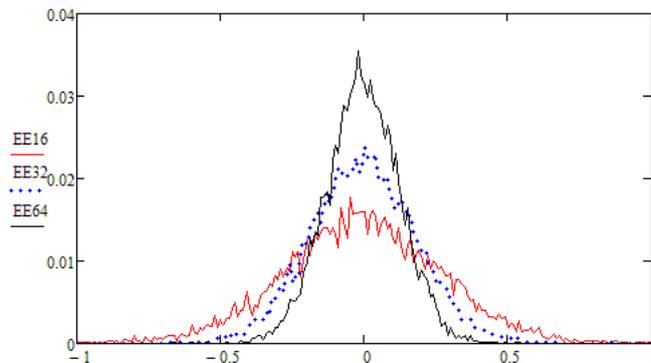


Ошибки вычисления математических ожиданий и стандартных отклонений из-за ограниченных малых выборок обучения

```

sx16(r) := | x ← sort(mom(16, 0, 1 + r))
           | x ←  $\frac{x}{\text{stdev}(x)}$ 
           | m ← mean(x)
           | m
           |
sx32(r) := | x ← sort(mom(32, 0, 1 + r))
           | x ←  $\frac{x}{\text{stdev}(x)}$ 
           | m ← mean(x)
           | m
           |
sx64(r) := | x ← sort(mom(64, 0, 1 + r))
           | x ←  $\frac{x}{\text{stdev}(x)}$ 
           | m ← mean(x)
           | m
           |

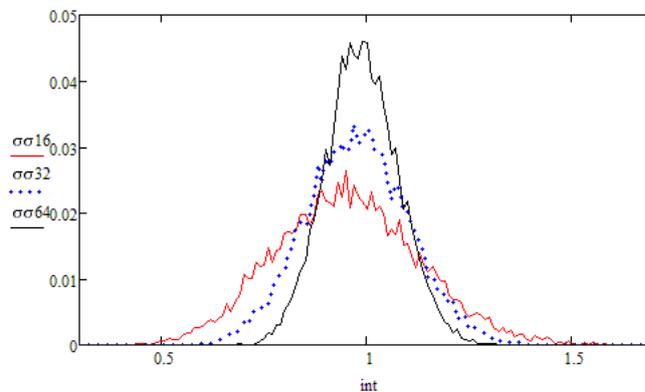
i := 0..9999   rri := md(0.01)   E16i := sx16(rri)   E32i := sx32(rri)   E64i := sx64(rri)
j := 0..999   intj := -1 + 0.01*j   EE16 :=  $\frac{\text{hist}(\text{int}, E16)}{9999}$    EE32 :=  $\frac{\text{hist}(\text{int}, E32)}{9999}$    EE64 :=  $\frac{\text{hist}(\text{int}, E64)}{9999}$ 
    
```



```

ss16(r) := | x ← sort(mom(16, 0, 1 + r))
           | x ← x - mean(x)
           | σ ← stdev(x)
           | σ
           |
ss32(r) := | x ← sort(mom(32, 0, 1 + r))
           | x ← x - mean(x)
           | σ ← stdev(x)
           | σ
           |
ss64(r) := | x ← sort(mom(64, 0, 1 + r))
           | x ← x - mean(x)
           | σ ← stdev(x)
           | σ
           |

i := 0..9999   rri := md(0.01)   σ16i := ss16(rri)   σ32i := ss32(rri)   σ64i := ss64(rri)
j := 0..999   intj := 0.3 + 0.01*j   σσ16 :=  $\frac{\text{hist}(\text{int}, \sigma16)}{9999}$    σσ32 :=  $\frac{\text{hist}(\text{int}, \sigma32)}{9999}$    σσ64 :=  $\frac{\text{hist}(\text{int}, \sigma64)}{9999}$ 
    
```



Ошибки вычисления коэффициентов корреляции из-за ограниченных малых выборок обучения

```

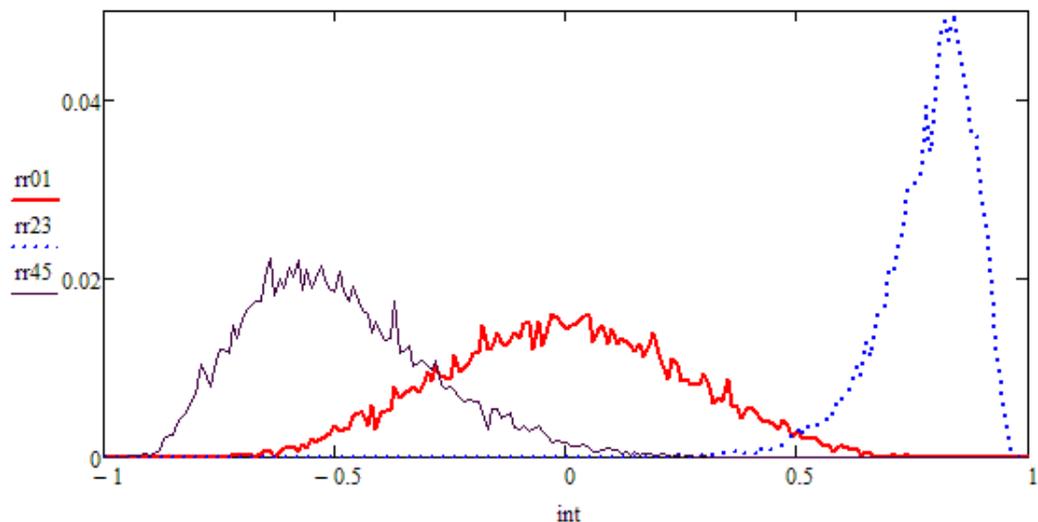
i := 0..9999      b := 1
a := 0.5    n := 16    zⓈ := momm(n,0,1)    x0Ⓢ := momm(n,0,1)    x1Ⓢ := momm(n,0,1)
x3Ⓢ := momm(n,0,1)    x2Ⓢ := momm(n,0,1)    x2Ⓢ :=  $\frac{a \cdot x2^{\text{Ⓢ}} + z^{\text{Ⓢ}}}{\sqrt{1+a^2}}$     x3Ⓢ :=  $\frac{a \cdot x3^{\text{Ⓢ}} + z^{\text{Ⓢ}}}{\sqrt{1+a^2}}$ 
x4Ⓢ := momm(n,0,1)    x5Ⓢ := momm(n,0,1)    x4Ⓢ :=  $\frac{b \cdot x4^{\text{Ⓢ}} - z^{\text{Ⓢ}}}{\sqrt{1+b^2}}$     x5Ⓢ :=  $\frac{b \cdot x5^{\text{Ⓢ}} + z^{\text{Ⓢ}}}{\sqrt{1+b^2}}$ 

corr(x0,x1) = 0.0014231      corr(x2,x3) = 0.8
                             corr(x4,x5) = -0.5

r01i := corr(x0Ⓢ,x1Ⓢ)      r23i := corr(x2Ⓢ,x3Ⓢ)      r45i := corr(x4Ⓢ,x5Ⓢ)

j := 0..9999    intj := -1 + 0.01·j    rr01 :=  $\frac{\text{hist}(\text{int}, r01)}{9999}$     rr23 :=  $\frac{\text{hist}(\text{int}, r23)}{9999}$     rr45 :=  $\frac{\text{hist}(\text{int}, r45)}{9999}$ 

```



Приложение 7

Пример блуждания, возникающего при вычислении математического ожидания и стандартного отклонения на большой выборке в 1000 опытов

`x := morm(1000,0,1) i := 1..999`

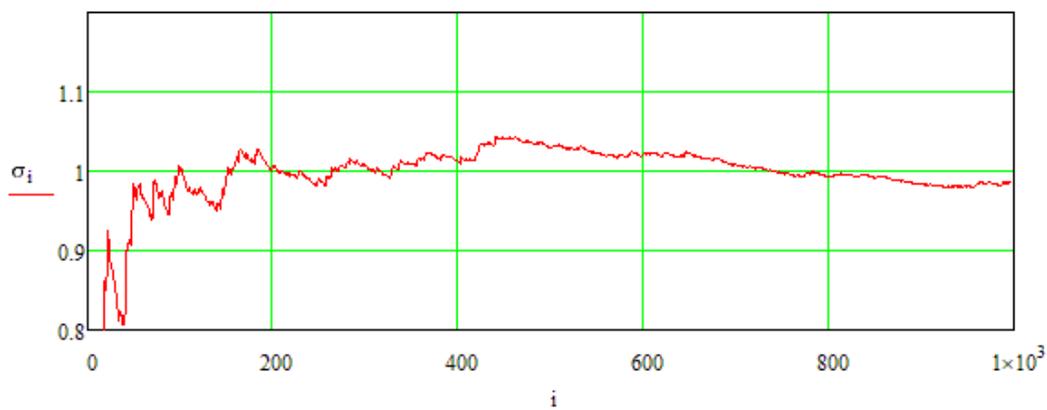
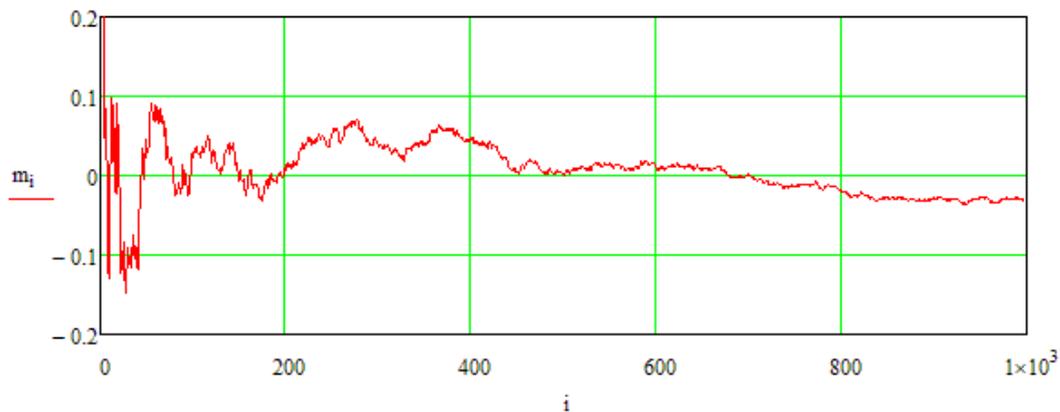
$$m_0 := x_0 \quad m_i := \frac{\left(m_{i-1} + \frac{x_i}{i}\right)}{1 + \frac{1}{i}} \quad \text{mean}(x) = -0.033 \quad m_{999} = -0.033 \quad \frac{0.1}{\sqrt{1000}} = 0.00316$$

`s_0 := 0`

$$s_i := \frac{\left[s_{i-1} + \frac{(m_i - x_i)^2}{i}\right]}{\left(1 + \frac{1}{i}\right)} \quad \sigma_i := \sqrt{s_i} \quad \frac{1 - 0.9}{\sqrt{1000}} = 0.003162$$

`stdev(x) = 0.99`

`σ999 = 0.987`



**Список ранее опубликованной литературы
издательствами «Пензенского
научно-исследовательского
электротехнического института»
и «Пензенского государственного университета»
по близкой тематике**

1. Иванов А. И., Захаров О. С. Среда моделирования «БиоНейро-Автограф». Программный продукт создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ» URL: <http://пниэи.рф/activity/science/noc/bioneuroautograph.zip> для свободного использования университетами России, Белоруссии, Казахстана.

2. Иванов А. И. Автоматическое обучение больших искусственных нейронных сетей в биометрических приложениях : учеб. пособие. Пенза, 2013. 30 с. URL: http://пниэи.рф/activity/science/noc/tm_IvanovAI.pdf

3. Иванов А. И. Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции. Пенза : Изд-во АО «ПНИЭИ». 2016. 133 с. URL: <http://пниэи.рф/activity/science/BOOK16.pdf>

4. Иванов А. И. Простейшие оракулы, обученные корректировать ошибки вычисления младших статистических моментов на малых выборках биометрических данных: учеб. пособие. Пенза : Изд-во АО «Пензенский научно-исследовательский электротехнический институт», 2018. 35 с. URL: <http://пниэи.рф/activity/science/noc/BOOK18.pdf>

5. Иванов А. И. Численная оценка показателей квантовой сцепленности выходных кубит нейросетевой молекулы преобразователя биометрических данных : учеб. пособие. Пенза, 2018. Пенза : Изд-во АО «Пензенский научно-исследовательский электротехнический институт» (АО «ПНИЭИ»), 2018. 27 с. URL: <http://пниэи.рф/activity/science/noc/BOOK18-2.pdf>

6. Иванов А. И. Искусственные математические молекулы: повышение точности статистических оценок на малых выборках (программы на языке MathCAD) : препринт. Пенза : Изд-во ПГУ, 2020. 36 с. ISBN 978-5-907262-42-3.

7. Иванов А. И. Исследование свойств нейросетевого преобразователя биометрия-код с использованием среды моделирования «БиоНейроАвтограф» : учеб.-метод. пособие. Пенза : Изд-во ПГУ, 2020. 40 с. URL:<https://tsib.pnzgu.ru/page/39329>

8. Иванов А. И. Среда моделирования «БиоНейроАвтограф» : учеб.-метод. пособие. Пенза : Изд-во ПГУ, 2020. 60 с. URL: <https://tsib.pnzgu.ru/page/39329>

9. Иванов А. И. Тестирование нейронных сетей, обученных алгоритмом ГОСТ Р 52633.5–2022, в среде моделирования «БиоНейроАвтограф» : учеб.-метод. пособие. Пенза : Изд-во ПГУ, 2020. 36 с. URL: <https://tsib.pnzgu.ru/page/39329>

10. 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. ISBN 978-5-907262-59-1

11. Иванов А. И., Куприянов Е. Н. Защита искусственного интеллекта : ортогонализация статистико-нейросетевого анализа малых выборок биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 72 с. ISBN 978-5-907262-72-0.

12. Иванов А. И., Золотарева Т. А. Искусственный интеллект в защищенном исполнении: синтез статистико-нейросетевых автоматов многокритериальной проверки гипотезы независимости малых выборок биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 105 с. ISBN 978-5-907364-24-0.

13. Малыгина, Е. А. Биометрико-нейросетевая аутентификация: перспективы применения сетей квадратичных нейронов с многоуровневым квантованием биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 114 с. ISBN 978-5-907262-88-1.

14. Иванов А. И., Сулавко А. Е. Использование сетей корреляционных нейронов с многоуровневым квантованием: защита от извлечения знаний из параметров решающего правила : препринт. Пенза : Изд-во ПГУ, 2020. 48 с. ISBN 978-5-907364-02-8.

15. Иванов А. И., Юнин А. П. Эмбрион искусственного интеллекта: компактная нейросетевая проверка качества случайных последовательностей, полученных из биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 48 с. ISBN 978-5-907364-80-6.

16. Иванов А. И., Иванов А. П., Ратников К. А. Статистико-нейросетевой анализ биометрических образов в пространствах спектров кроссверток и автосверток Хэмминга. Пенза : Изд-во ПГУ, 2021. 56 с. ISBN 978-5-907364-94-3.

17. Иванов А. И. Высокоразмерная коллективная биометрия подсознательного поведения людей на рынке и производстве : препринт. Пенза : Изд-во ПГУ, 2021. 60 с. ISBN 978-5-907456-44-0.

Научное издание

Иванов Александр Иванович

**НЕЙРОДИНАМИКА: ГИПЕРУСКОРЕНИЕ
НАПРАВЛЕННЫХ ПЕРЕБОРОВ ИЛИ ПОВЫШЕНИЕ
ДОСТОВЕРНОСТИ СТАТИСТИЧЕСКИХ ОЦЕНОК
НА МАЛЫХ ВЫБОРКАХ**

Редактор *Е. В. Шмелева*

Технический редактор *Ю. В. Анурова*

Компьютерная верстка *Ю. В. Ануровой*

Дизайн обложки *А. А. Стаценко*

Подписано в печать 22.09.2021.

Формат 60×84¹/₁₆. Усл. печ. л. 6,16.

Заказ № 455. Тираж 300.

Издательство ПГУ

440026, Пенза, Красная, 40.

Тел. 66-60-49, 66-67-77; e-mail: iic@pnzgu.ru

