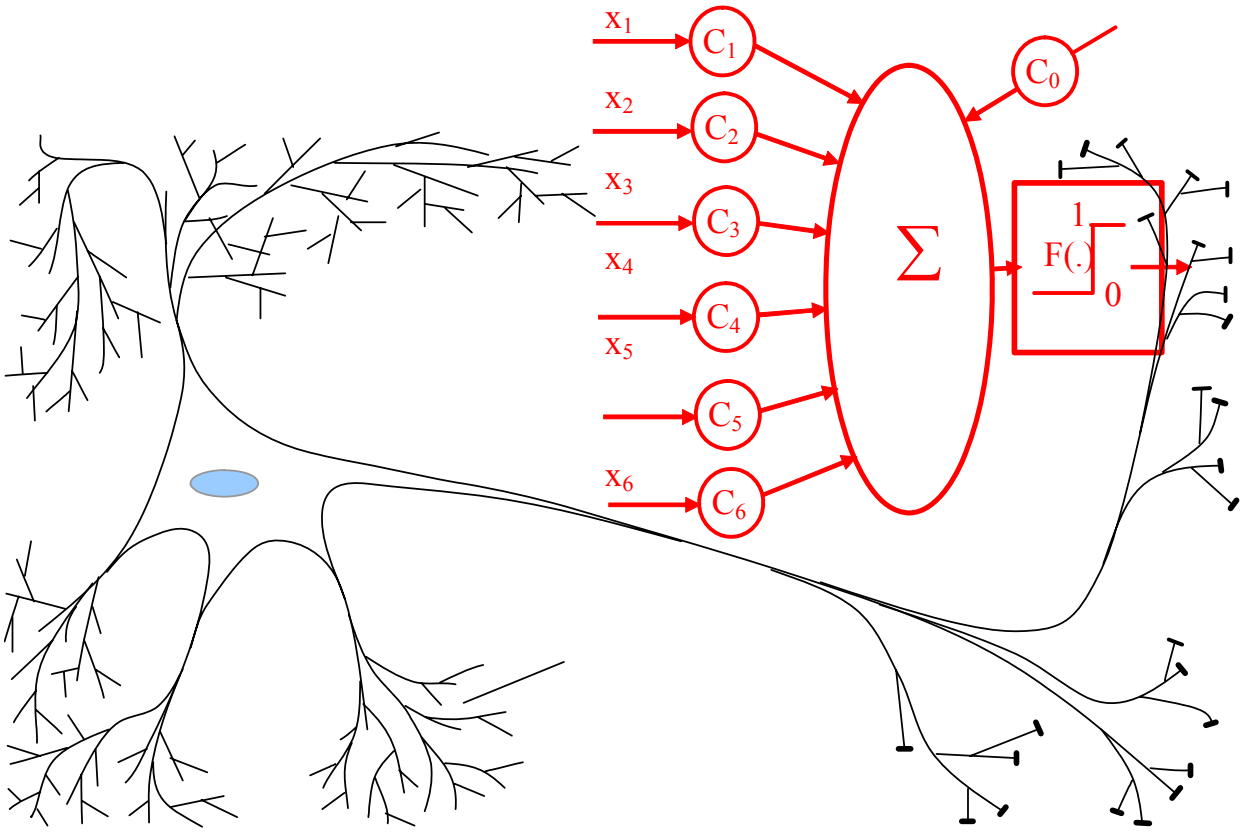
УДК: 004.8; 519.7; 57.087.1; 621.391; 681.5
Электронная книга издательства ОАО «ПНИЭИ»
http://пниэи.рф/activity/science/bio_neuro.pdf

Иванов А.И.

ПОДСОЗНАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРОГРАММИРОВАНИЕ АВТОМАТОВ НЕЙРОСЕТЕВОЙ БИОМЕТРИИ ЯЗЫКОМ ИХ ОБУЧЕНИЯ



Россия, Пенза- 2012

УДК: 004.8; 519.7; 57.087.1; 621.391; 681.5

Электронная книга издательства ОАО «ПНИЭИ» под экран от 7” и выше, 125 с.
http://пниэи.рф/activity/science/bio_neuro.pdf

Подсознание искусственного интеллекта: программирование автоматов нейросетевой биометрии языком их обучения

Рассматривается одно из направлений развития искусственного интеллекта. Показано, что новый алгоритм быстрого автоматического обучения больших искусственных нейронных сетей отечественного стандарта ГОСТ Р 52633.5-2011 имеет линейную вычислительную сложность и, как следствие, снимает ограничения на размерность решаемых задач. Отпадает необходимость в полной формализации задач перед их решением. Для поиска нужного нейросетевого решения достаточно иметь не более 20 примеров распознаваемого образа. Выдвинута гипотеза о том, что подсознание естественных нейронных сетей человека работает на похожих принципах и способно решать задачи высокой и сверхвысокой размерности. Даны сравнительные оценки размерности задач, решаемых сознательной и подсознательной частью искусственного интеллекта автоматов, а так же сознательной и подсознательной частью естественного интеллекта человека.

Сведения об авторе: Иванов Александр Иванович, д.т.н., доцент, начальник лаборатории биометрических и нейросетевых технологий ОАО «Пензенский научно-исследовательский электротехнический институт»

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Интеллект – это главное, чем люди отличаются от животных. Однако то, что в языке называется «интеллект», является весьма и весьма сложным социально-культурным понятием. С одной стороны, каждый из нас обладает некоторым интеллектом и гордится им, осознавая себя именно человеком, но, с другой стороны, наш личный интеллект является еще и общественным достоянием (продуктом). Это легко доказывается эффектом «Маугли». Маленький ребенок, попав в стаю волков становится волком и своим развитым «человеко-волчьим» интеллектом решает насущные задачи своей стаи.

Чем мы думаем и как мы это делаем давно заботит человечество. Еще древние философы научились выявлять формальную логику рассуждений и выводов. Важнейший вклад в понимание ограниченности нашего интеллекта внес средневековый английский философ Уильям Оккам. В 13 веке он сформулировал принцип «бритвы Оккама» (не следует преумножать число сущностей сверх необходимого).

Руководствуясь принципом «бритвы Оккама» человечество успешно справлялось со своими научно-технологическими задачами в течение 700 лет. Во времена средневековья и индустриализации необходимо было упрощать задачу настолько, насколько это возможно, и тем самым облегчать ее для решения человеком (понимания человеком). Все это абсолютно правильно для предшествующих эпох неавтоматизированного умственного труда людей (неинтеллектуальных средств добычи знания и производства материальных благ).

В середине прошлого века с появлением первых ЭВМ ситуация начала изменяться. Мы все стали свидетелями того, что вычислительные машины постепенно стали брать на себя функции естественного интеллекта человека. Еще вчера вычислительные машины умели играть в шахматы, но проигрывали обычным людям. Сегодня обычный человек уже не способен обыграть в шахматы обычную шахматную программу, поставленную на обычный компьютер. Более того, люди в лице чемпиона мира по шахматам проигрывают специально созданным шахматным программам.

Параллельно с развитием средств вычислительной техники возникло новое быстро развивающееся научное направление исследований - искусственный интеллект. По закону Мура вычислительное железо постоянно дешевеет, параллельно увеличивая свои возможности. То же самое происходит и с программными приложениями, размеры их текстов экспоненциально растут и казалось бы, что должны экспоненциально расти и их возможности. На самом деле этого не происходит: интеллектуальные возможности программного обеспечения растут много медленнее, чем размеры их текстов. Искусственный интеллект добился ощутимых успехов только в изначально хорошо формализованных приложениях. Игра в шахматы является хорошо формализованной задачей, и именно по этой причине, наращивание вычислительных ресурсов дает возможность машине просматривать большее число ходов игры и в конечном итоге обыгрывать человека. Если задача не поддается формализации, то сегодняшний искусственный интеллект начинает

хромать и не может переиграть человека.

Тупиковая ситуация с плохо формализуемыми задачами сдвинулась с мертвой точки только в начале этого 21 века. Прорыв создала Россия в приложениях биометрической аутентификации. Образ человека размыт и не поддается формальному описанию, мы легко решаем задачи распознавания образов знакомых нам людей. Машины этого делать ранее не умели, но быстро научились после того как их искусственный интеллект был снабжен большими искусственными нейронными сетями. Размер искусственной нейронной сети биометрического автомата существенно влияет на его интеллектуальные возможности. Очевидно, что маленькие искусственные нейронные сети обеспечивают низкую интеллектуальность машины, а большие искусственные нейронные сети должны потенциально обеспечивать более высокий уровень интеллектуальности.

В связи со столь простой зависимостью размеров искусственной нейронной сети и интеллектуальных возможностей машины, имеет смысл отказаться от экономии числа искусственных нейронов и не экономить на числе обрабатываемых искусственной нейронной сетью параметров. В прошлом веке этого делать было нельзя, так как вычислительные машины были маленькими и, самое главное, отсутствовали эффективные алгоритмы обучения искусственных нейронных сетей. В этом веке вычислительные машины стали обладать достаточными ресурсами, и появились алгоритмы автоматического обучения больших искусственных нейронных сетей (описание алгоритмов дано в ГОСТ Р 52633.5-2011).

Это означает, что применительно к задачам биометрической аутентификации личности «бритва Оккама» перестала работать. Нам уже нет необходимости экономить на размерности решаемой задачи и на сложности алгоритма ее решения (числе слоев нейронов сети и числе связей между нейронами). Теоретически мы имеем возможность наращивать размерность задачи (число учитываемых параметров) до того момента, пока задача не утратит своей изначальной случайной составляющей.

В этом плане биометрия является хорошим примером. Пока мы пользуемся «бритвой Оккама» и учитываем малое число только «очень хороших» биометрических параметров задача плохо решается (решение имеет значительную случайную составляющую). Происходит это из-за того, что «очень хороших» биометрических параметров всегда мало. Просто «хороших», «удовлетворительных», «плохих» и «очень плохих» биометрических параметров в сотни и даже тысячи раз больше, чем «очень хороших».

Если отказаться от принципа «бритвы Оккама», перестать экономить и учитывать все параметры, то удается добиться значительного повышения качества принимаемых нейронной сетью решений. При этом, для обучения нейронной сети подходит далеко не каждый из известных алгоритмов. Алгоритм обучения должен быть очень устойчивым (работать со входными биометрическими данными любого качества), кроме того, алгоритм должен сохранять свою устойчивость при использовании нейронной сетью очень большого числа входных параметров. Алгоритмы обучения, описанные в ГОСТ Р 52633.5-2011, как раз и

обладают высокой устойчивостью при неограниченно большом числе входных параметров нейронной сети.

Необходимость в написании данной книги обусловлена тем, что отечественные стандарты серии ГОСТ Р 52633.xx-20xx формально распространяются только на средства высоконадежной биометрической аутентификации. Для решения других задач (трехмерное зрение, прогнозирование состояний рынка, прогнозирование погоды, оценка рисков появления сложных событий,….) нейросетевые решения так же должны оказаться работоспособными. Однако адаптация знаний, уже полученных при решении биометрических задач, не всегда тривиальна; при решении каждого нового класса задач появляется масса специфических особенностей. Сегодня можно говорить только о возможности переноса общих принципов уже созданных нейросетевых биометрических решений на аналогичные нейросетевые решения в других областях знаний.

Уважаемого читателя я прошу отнестись достаточно скептически к тому, что изложено в данной книге. Однако, если даже половина того, что изложено в книге, подойдет для других приложений, цель будет достигнута. Необходимо как можно быстрее попытаться перенести передовой опыт создания высоко-размерных нейросетевых биометрических приложений в иные прикладные решения. Существенное увеличение размерности решаемых прикладных задач (увеличение размерности прикладного искусственного интеллекта) всегда должно давать значительное повышение качества принимаемых машинами решений.

1. Размерность решаемых задач в качестве показателя различия между сознанием и подсознанием естественного (искусственного) интеллекта

В литературе прошлого века достаточно часто встречается утверждение о том, что мы, люди, используем возможности своего мозга не более чем на 3%. Я лично к подобным высказываниям отношусь как к глупости. Мозг – это один из самых эффективных наших органов и он используется на все 100%. Во время голодания, когда идет само поедание организмом всех органов, сохраняют свой вес только мозг и сердце. Все остальные органы, существенно утрачивают свой вес, организм ими жертвует.

Жертвовать мозгом нельзя, весь остальной организм занимается обслуживанием именно мозга. Первые 21 день после нашего зачатия наш организм развивается экспоненциально (происходит взрывное деление клеток) мы из ничего превращаемся в рисовое зернышко. Как только в зернышке зародыша намечается головка и спинной мозг, взрывное деление клеток прекращается. Далее рост организма строго синхронизован с потребностями мозга. У разных видов млекопитающих разные мозги и, соответственно, разная скорость роста их детенышей. Тигренок к трем годам становится огромным тигром (ему это позволяет его мозг), а человеческий ребенок в три года остается маленьким. В этом возрасте ребенок хорошо говорит и начинает активно учится заполнять сознательную составляющую своего интеллекта. Только к 18 годам граждане России догоняют по росту и сознанию своих родителей, становятся полноправным членами

общества, могут вступать в брак и заводить своих детей. Наши дети растут и взрослеют в шесть раз медленнее тигрят и в девять раз медленнее котят.

Байка о 3% использования интеллекта, скорее всего, обусловлена наличием у человека сознания и подсознания. Примерно 3% от объема головного мозга человека занимает его кора, где размещается то, что мы называем сознанием. Все, что находится под корой, является глубинами **под**сознания человека. Наше собственное сознание относительно понятно для нас и порождает иллюзию своей доступности. Наше подсознание много мощнее и эффективнее нашего сознания, но оно нам абсолютно недоступно и непонятно. Загрузка нашего сознания и подсознания полная на все 100%, но воспринимается нами только как 3% из-за нашей способности оценивать (контролировать) только работу сознательной части естественного интеллекта.

Работа сознательной части нашего интеллекта неразрывно связана с тем языком, на котором мы думаем. Соответственно, размерность задач, решаемых нашим сознанием, можно оценить через статистические параметры языка, на котором сознание осуществляет постановку задач и формулирует выработанное им решение.

Например, мы можем воспользоваться статистиками языка записи множества шахматных партий. Каждую шахматную партию можно записать в виде последовательности ходов передвижения белых и черных фигур по шахматной доске с момента дебюта до окончания партии. Для подобных записей можно рассчитать энтропию языка шахматных текстов и, соответственно, вычислить

размерность задачи, решаемой игроком средней руки или мастером. Если обычный игрок просматривает последствия своих действий только на три хода, то размерность решаемой им задачи будет совпадать с энтропией трех ходов записей шахматных партий. Для мастера способного просчитывать шахматную ситуацию на 9 ходов, энтропия решаемых им задач (их размерность) будет в 3 раза выше. Трехкратное увеличение размерности решаемых мастером шахматных задач дает ему возможность обыгрывать шахматиста средней руки. Однако, если мастер будет иметь дело с шахматной машиной, способной просматривать цепочки из 12 ходов, то он с достаточно высокой вероятностью будет проигрывать партии в шахматы искусственному интеллекту.

Выше описан достаточно простой способ оценки размерности задач, решаемых нашим с вами естественным сознательным интеллектом и искусственной частью сознательного интеллекта шахматной машины. Сомневаться в технической реализуемости подобного способа оценки нет причин, однако, убивать время на его реализацию жалко. В связи с этим, упростим задачу и заменим произвольный шахматный текст на произвольный текст английского языка. Средняя длина слова текстов на английском составляет 5.5 букв, каждая буква имеет энтропию 1,3 бита. При таком упрощении шахматист средней руки будет предугадывать следующие три слова описания текущей партии или решать задачи размерностью 21 бит (с 21 независимыми переменными), а мастер будет способен решать шахматные задачи с размерностью в 63 независимые переменные.

Для того, что бы оценить размерность задач, решаемых нашим **под**сознанием, проанализируем ситуацию, когда мы рассматриваем лицо человека, пытаясь его узнать. При этом мы задействуем два глаза, каждый из которых имеет на задней стенке по 120 миллионов специальных нервных клеток - палочек и 6 миллионов нейронов - колбочек. То есть, 126 миллионов чувствительных к свету нейронов могут давать поток из 126 миллионов откликов, изменяющих свое состояние с частотой 100 Герц. Этот поток поступает на другие нейроны – обработки зрительной информации, которые могут иметь до 10 тысяч входов. Если наша система естественной биометрической идентификации крайне примитивна и способна различать не более одного образа «Свой», то она должна быть как минимум 10 000-мерной (один нейрон с 10 000 входами принимает решение «Свой» или «Чужой»). Если у человека более сложная система идентификации личности, способная запоминать лица до 1000 знакомых людей, то ее размерность должна оказаться существенно выше, чем 10 000.

Приведенные выше оценки достаточно надежно показывают разницу между возможностями нашего сознания и возможностями нашего **под**сознания. Сознание среднестатистического игрока в шахматы способно решать не более чем 7-ми мерные задачи. Наиболее глупые из нас способны решать задачи в трое меньшей размерности, а самые умные из нас способны решать задачи в трое более высокой размерности. Но независимо от эффективности нашего сознания, каждый из нас имеет подсознание, способное справляться с задачами, имеющими размерность 10 000 и более.

Важнейшим моментом является то, что сознание и **под**сознание являются совершенно разными фрагментами естественного интеллекта и искусственного интеллекта. Люди и машины, показывающие низкие результаты при тестировании их сознания (осознаваемых и понимаемых людьми функций), могут иметь очень высокие результаты при тестировании возможности их **под**сознания. Маугли, воспитанный волчьей стаей, видимо, будет получать низкие оценки своих умственных способностей от своих цивилизованных сверстников. Однако, он будет уметь выполнять то, что его цивилизованные сверстники сделать не способны в принципе. При этом, Маугли будет плохо говорить, но даже, если бы он смог очень хорошо говорить, объяснить, то как он делает уникальные вещи, он не сможет. Любой из спортивных чемпионов умеет делать то, что не могут другие, но объяснить как он это делает невозможно. Мы ходим, говорим, плаваем, дышим, видим, бегаем, сражаемся в поединках опираясь на наше высоко-размерное **под**сознание. Найти собственное решение очень сложной реальной задачи (самостоятельно или под руководством тренера) на много реальнее, чем потом объяснить то, как ты это делаешь. До 97% наших интеллектуальных ресурсов уходит на **под**сознательный поиск верного высоко-размерного решения, сформулировать найденные нами самостоятельно высоко-размерные решения средствами низко-размерного языка и передать эти знания другим людям очень трудно, почти невозможно. Знают через умение многие, формализовать свои знания и объяснить другим могут только гении. Подчас гениям приходится прибегать к модификации языка общения

(придумывать свои слова или даже создавать новый язык), для того, чтобы объяснить другим людям взаимодействие с новыми сущностями.

2. Слова естественного языка общения людей как результат перевода высоко-размерной аналоговой действительности в цифровые формы более низкой размерности

Принципиальное отличие людей от других млекопитающих животных в наличии у людей развитого языка взаимного общения. Общаясь на своем языке люди передают друг другу значительные объемы важной информации. Язык – это средство формализации знаний с целью передачи информации другим людям или получения информации от других людей. Естественный язык взаимного общения является итогом коллективного творчества. Овладение уже созданным языком каждым новым человеком является самостоятельным творческим актом со стороны овладевающего.

Синтез и овладение языком строятся на примерах. Чтобы овладеть понятием «человек» обучаемому следует предъявить 20-30 разных людей (разного пола, разного возраста, разных рас). Обучаемый сам должен выделить то общее, что сближает людей и отличает их от всех других живых существ. Как это делает каждый из нас (какие и сколько признаков людей используются) никто точно ответить не может. Скорее всего, у каждого из нас имеется своя не формализованная система из нескольких сотен признаков человека, отличающих людей от просто животных.

Естественно, что у обучаемого уже должна иметься база

примеров образов всех других живых существ. Таких образов примеров «живых существ» может быть несколько сотен или даже тысяч. Все это повторяет процедуры обучения искусственных нейронных сетей распознаванию образа «Свой» на фоне нескольких сот биометрических примеров образов «Чужие» по ГОСТ Р 52633.5-2011. По своей сути биометрическая идентификация конкретного человека «Свой»-«Чужой» является уточнением процедуры классификации более высокого уровня «человек»-«животное» или еще более высокого уровня классификации «живое»-«неживое».

При обучении языковой классификации каждому выделяемому классу живых существ люди присваивают свой звуковой код «человек», «тигр», «олень», «медведь»,….. Таких классов в том или ином естественном языке существует несколько тысяч (по числу наблюдаемых людьми живых существ). И здесь наблюдается полная аналогия с автоматическим обучением искусственной нейронной сети по ГОСТ Р 52633.5-2011, требующему еще до обучения присвоить выделяемому классу «Свой» личный код доступа.

Фактически, короткий звуковой код (название животного) ставится в соответствие его многомерному непрерывному (аналоговому) образу этого животного (этого класса животных). Получается, что язык – это средство короткого цифрового описания очень сложной аналоговой действительности. Каждый человек в реальной действительности имеет дело с очень сложными высоко-размерными непрерывными образами окружающих предметов, отображаемыми в языке их короткими

кодами-названиями. В этом отношении язык – это форма эффективного сжатия информации для передачи ее соседу или для получения ее от соседа. Получается, что первая цифровая революция произошла несколько десятков тысяч лет назад, когда наши предки создали для себя праязык. Звуки того или иного языка являются первыми цифровыми кодами, созданными для цифровых коммуникаций между людьми. Когда мы учимся произносить слова языка, мы учимся кодировать наши знания на том или ином языке. Когда мы учимся понимать язык, мы учимся декодировать информацию, воспроизведенную на том или ином языке.

Запись языка на бумаге с помощью рукописных или печатных букв есть не что иное как вторичное перекодирование информации звуко-кодов мягкой воздушной среды в кодо-буквы с целью перенесения информации на какой-либо твердый носитель. Размерность кодо-слов языка всегда много ниже размерности задач, решаемых подсознанием при связывании реальных образов с их кодами-словами.

3. Информационная мера качества исходных данных

Данные бывают «плохого» и «хорошего» качества, мы все это понимаем на интуитивном уровне. Одним из формальных способов оценки качества данных является вычисление их энтропии по Шеннону [1, 2, 3]. Шеннон исследовал речь человека, воспроизведенную на некотором естественном языке и уже оцифрованную на некотором алфавите из S букв, представленную в виде текста. Любой человек, знающий язык и обученный

алфавиту легко читает текст и понимает его смысл. Машины во времена Шеннона, да и в наше время, видят только оболочку знаний в виде последовательности букв текста. Машинам доступна операция по оценке энтропии появления одиночных символов алфавита в тексте:

$$H(x_1) = -\sum_{1i=1}^{S} P(x_{1i}) \cdot \log_2(P(x_{1i})) = \sum_{1i}^{S} P(x_{1i}) \cdot I(x_{1i}) \qquad (1),$$

где $P(x_{1i})$ - вероятность появления одиночного i-го символа в тексте, принадлежащего алфавиту из S символов, $I(x_{1i}) = -\log_2(P(x_{1i})$ информация, получаемая при появлении i-го символа.

Очевидно, что рассматривая каждую из букв текста независимо от других букв понять смысла текста нельзя. В связи с этим энтропия первого порядка (1) должна быть заменена энтропиями более высоких порядков. Формулы для расчета энтропий более высокого порядка строятся по индукции:

$$H(x_1, x_2) = -\sum_{1i=1}^{S}\sum_{2i=1}^{S} P(x_{1i}, x_{2i}) \cdot \log_2(P(x_{1i}, x_{2i})) = \sum_{1i=1}^{S}\sum_{2i=1}^{S} P(x_{1i}, x_{2i}) \cdot I(x_{1i}, x_{2i})) \quad (2);$$

.....;

$$H(x_1, x_2, ..., x_n) = \sum_{1i=1}^{S}\sum_{2i=1}^{S} .... \sum_{ni=1}^{S} P(x_{1i}, x_{2i}, ..., x_{ni}) \cdot I(x_{1i}, x_{2i}, ..., x_{ni}) \quad (3);$$

.....;

где $P(x_{1i}, x_{2i}, ..., x_{ni})$ - вероятность появления некоторой n-граммы из n символов в исследуемом тексте, принадлежащих алфавиту из S символов, $I(x_{1i}, x_{2i}, ..., x_{ni})$ - информация при получении сочетания символов.

Следует подчеркнуть, что многомерная энтропия $H(x_1, x_2, ..., x_n)$ и многомерная информация $I(x_{1i}, x_{2i}, ..., x_{ni})$ это плод некоторых теоретических измышлизмов, воспользоваться которыми на практике достаточно сложно. При попытках осуществления прямых вычислений вида (3) требуются огромные затраты вычислительных ресурсов и очень большие объемы исходных текстов. Прямое вычисление многомерной энтропии нецелесообразно, однако косвенное (неявное) вычисление оценок энтропии того или иного порядка – это очень эффективный подход к решению множества задач.

Одной из проблем, с которой приходится сталкиваться при оценках энтропии и информации является то, что они хорошо вычислимы только на уже оцифрованных данных. Если исходные данные не оцифрованы (непрерывные), то вычисления вида (1), (2), (3) выполнить практически невозможно из-за отсутствия информации о многомерных распределениях значений непрерывных данных. Для того, чтобы обойти эту проблему рассмотрим простейшие процедуры оцифровки непрерывных данных в рамках примитивного алфавита, состоящего всего из двух значений «Свой» - «1» и «Чужой» - «0». Такой подход характерен для биометрических приложений.

Применительно к некоторому непрерывному биометрическому параметру - ξ_1 мы заранее знаем распределение все «Чужие» и можем найти распределение этого параметра для образа «Свой». В качестве контролируемого биометрического параметра ξ_1, например, может быть использован рост идентифицируемого

человека, измеренный видеокамерой. Типичное соотношение между распределением значений образов все «Чужие» и образа «Свой» по контролируемому биометрическому параметру - ξ_1 приведено на рисунке 1.

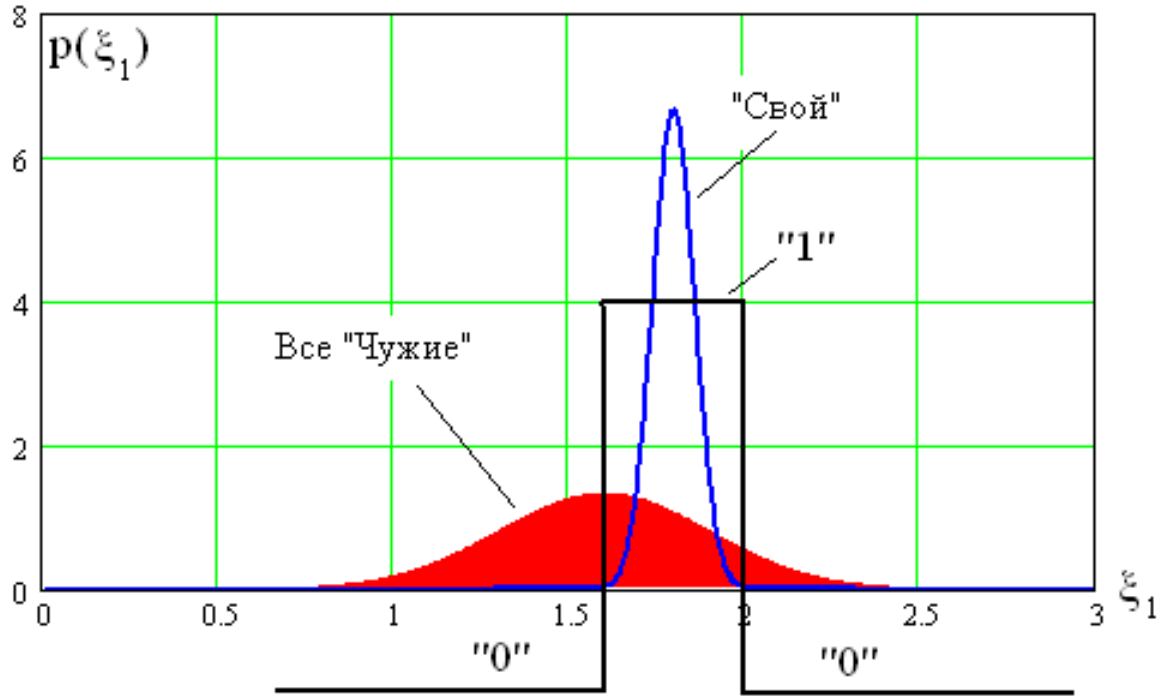


Рис. 1. Плотности распределения значений все «Чужие» и «Свой» роста человека - ξ_1, измеряемого видеокамерой

Из рисунка 1 видно, что видеокамера позволяет оценивать рост человека со значительной погрешностью из-за неопределенности расстояния до объекта а так же вариаций высоты каблуков и прически (головного убора). Все эти вариации приводят к тому, что интервал возможного изменения параметра - ξ_1 оказывается достаточно велик, однако, мы вполне можем его найти экспериментально при обучении средства и далее оценить энтропию контролируемого показателя:

$$H(\xi_1) \approx -\sum_{1i=0}^{1} P(\xi_{1i}) \cdot \log_2(P(\xi_{1i})) = \sum_{1i=0}^{1} P(\xi_{1i}) \cdot I(\xi_{1i})) \qquad (4),$$

где $P(\xi_{1,1})$- вероятность принятия решения «Свой» - состояние «1» при анализе единственного параметра - ξ_1;

$P(\xi_{1,0})$- вероятность принятия речения «Чужой» - состояние «0» при анализе единственного параметра - ξ_1.

Очевидно, что качество того или иного биометрического параметра -ξ_i будет тем выше, чем меньше его вариации и чем дальше распределение «Свой» вытолкнуто на периферию распределения все «Чужие». На роль меры качества ξ_1 пригодна информация, получаемая при наблюдении этого параметра:

$$I(\xi_1) = -\log_2(P(\xi_{1,1})) \qquad (5).$$

Информация (5) и энтропия (4) – это понятия противоположные друг другу. Информация это мера определенности, тогда как энтропия это мера неопределенности. Формально мы можем по индукции перейти к вычислению двухмерной энтропии $H(\xi_1,\xi_2)$ и двухмерной информации $I(\xi_1,\xi_2)$ и далее к вычислению многомерной энтропии $H(\xi_1,\xi_2,\ldots, \xi_n)$ и информации $I(\xi_1,\xi_2,\ldots, \xi_n)$. Однако, в этом нет смысла так как столь примитивный переход к цифровой форме от непрерывных параметров не конструктивен.

4. Как выглядит «проклятие размерности» в биометрических приложениях

Если воспользоваться соотношением (5) и рассчитать информацию 1024 параметров динамики рукописного слова-пароля [4, 5] (1024 коэффициентов двухмерного преобразования Фурье от двух связанных друг с другом кривых колебаний пера X(t),

Y(t)), то мы получим кривую упорядоченных показателей качества, приведенную на рисунке 2. Упорядочивание производилось так, что бы первыми оказались параметры с показателями наиболее высокого качества, а далее следовали показатели с убывающим качеством.

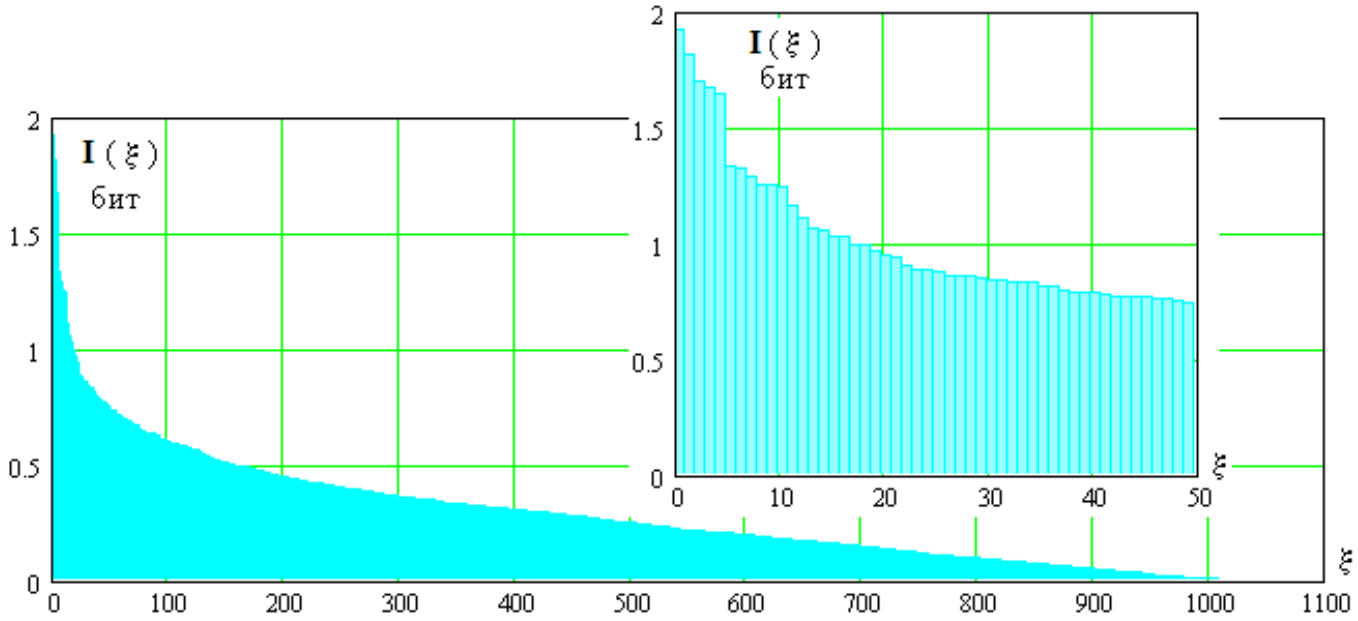


Рис. 2. Упорядоченные информационные показатели качества 1024 биометрических параметров рукописного образа «Свой»

Из рисунка 2 видно, что вектор контролируемых параметров содержит только 20 относительно «хороших» параметров с энтропий более одного бита. Остальные 1004 параметра относятся к «плохим» данным и имеют показатель качества существенно ниже одного бита.

Если бы мы имели «идеальный» алгоритм совместной обработки всех 1024 параметров (или все эти 1024 контролируемых параметров были бы независимыми), конечный результат можно было бы получить простым сложением всех информационных показателей качества. В этом случае мы получили бы кривую роста качества принимаемых решений по

мере учета все большего и большего числа параметров с монотонно убывающим качеством, приведенную на рисунке 3.

Из рисунка 3 видно, что учет идеальной машиной принятия решений всех хороших и всех плохих данных дает фантастически хорошее качество принятия решений. Триста бит дает вероятность появления ошибок на уровне 10^{-90} (десять в минус 90 степени). Если же мы воспользуемся «бритвой Оккама» и отрежем 1004 относительно плохих параметра (оставим 20 самых хороших), то можем получить информационный показатель качества на уровне 29 бит или ошибки будут появляться с вероятностью 10^{-8} (десять в минус 8 степени). Пользуясь привычной для нас «бритвой Оккама» мы потенциально теряем 82 порядка. Именно такие катастрофические потери ждут всех тех, кто хочет и дальше пользоваться «абсолютно правильными» понятиями прошлого века, выбирая только наиболее «информативные» параметры и катастрофически занижая размерность решаемых задач. Куда более правильным является завышение размерности задач и использование специально созданных нейросетевых решений, способных учитывать как хорошие, так и очень плохие данные.

Идеальной машины обогащения «плохих» и «очень плохих» данных создать невозможно. Речь может идти только о том, чтобы поднять информационной КПД с 3%, характерных для традиционных обогатителей данных, хотя бы до 20%, характерных для нейросетевых преобразователей биометрия-код [6], автоматически обученных по отечественному национальному стандарту ГОСТ Р 52633.5-2011 [7] (тонкая линия на рисунке 3).

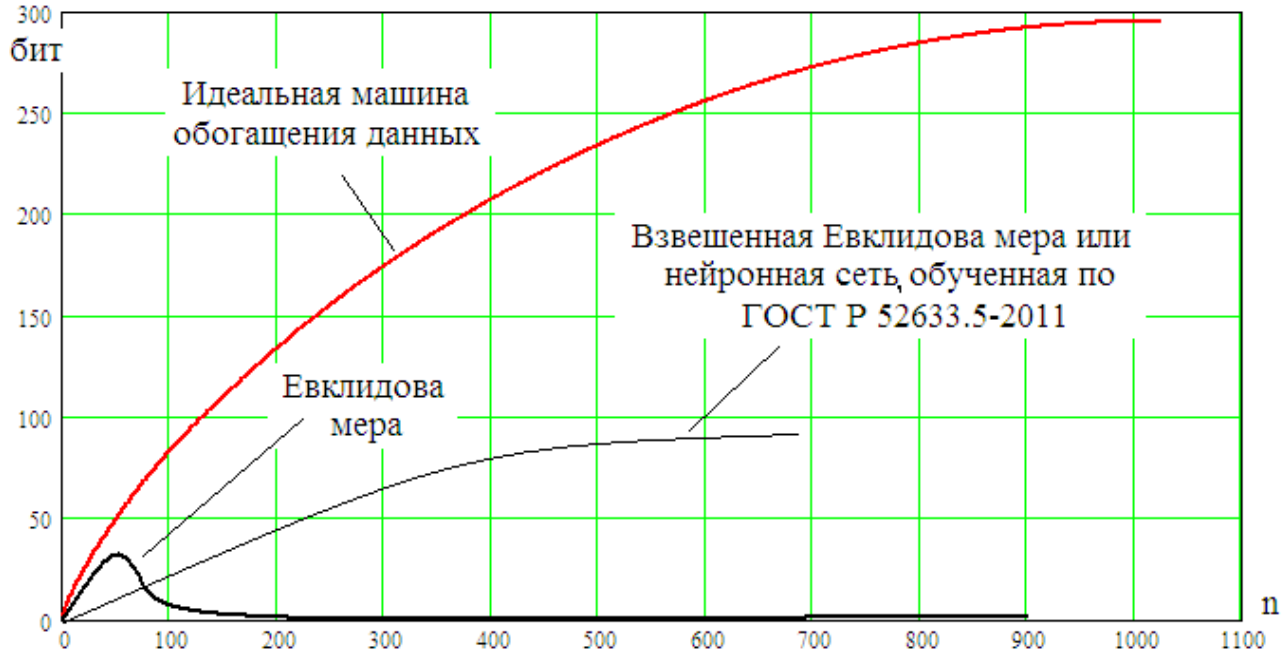


Рис. 3. Монотонный рост качества для идеальной машины обогащения (толстая линия) и для обычного вычисления Евклидовой меры и нейронной сети, обученной по ГОСТ Р 52633.5-2011 (тонкая линия)

Внешне «проклятие размерности» наблюдается как появление некоторого максимума меры качества, наблюдающегося при учете примерно 30 наиболее качественных биометрических параметров. После прохождения максимума показателя качества начинается монотонный спад качества, принимаемых решений за счет того, что алгоритм обогащения накапливает ошибки. При попытках учесть более 200 параметров «хорошего» и «плохого» качества обычная Евклидова мера перестает работать. Обычные Евклидовы обогатители данных при учете 200 и более параметров:

$$e = \sqrt{\frac{1}{200}\sum_{i=1}^{200}(\xi_i - E(\xi_{i,Свой}))^2} \qquad (6),$$

где $E(\xi_{i,Свой})$ - математическое ожидание i-го биометрического параметра образа «Свой»;

не могут надежно различать множества «Свой» и «Чужой». Их

показатель качества становится примерно равным одному биту ($P_{EE}=P_1=P_2 \approx 0.5$). То есть, в место вычислений по формуле (6) можно просто обращаться к генератору равновероятных псевдослучайных чисел.

Для того, чтобы обойти «проклятие размерности», необходимо от обычной меры Евклида переходить к взвешенной мере Евклида:

$$e = \sqrt{\frac{1}{1024}\sum_{i=1}^{1024}\mu_i \cdot (\xi_i - E(\xi_{i,Свой}))^2} \qquad (7).$$

Правильно выбранные весовые коэффициенты - μ_i делают решение устойчивым, при этом, проблема упирается именно в правильный выбор этих стабилизирующих решение весовых коэффициентов. Одним из путей определения стабилизирующих весовых коэффициентов - μ_i является переход к использованию алгоритмов обучения радиальных искусственных нейронных сетей [8]. Если отказаться от возведения в квадрат компонент взвешенной Евклидовой, то при поиске весовых коэффициентов мы придем к задаче обучения персептрона [4, 5, 6, 7].

5. Итерационное обучение искусственного нейрона с малым числом входов

Сегодня под искусственным нейроном подавляющее большинство авторов понимает сумматор с выходной нелинейностью. Нелинейность может иметь разную форму, мы далее будем рассматривать только пороговые нелинейные элементы. Нейроны с такими элементами иногда называют персептронами. Пример такого нейрона с 7 входами приведен на

рисунке 4.

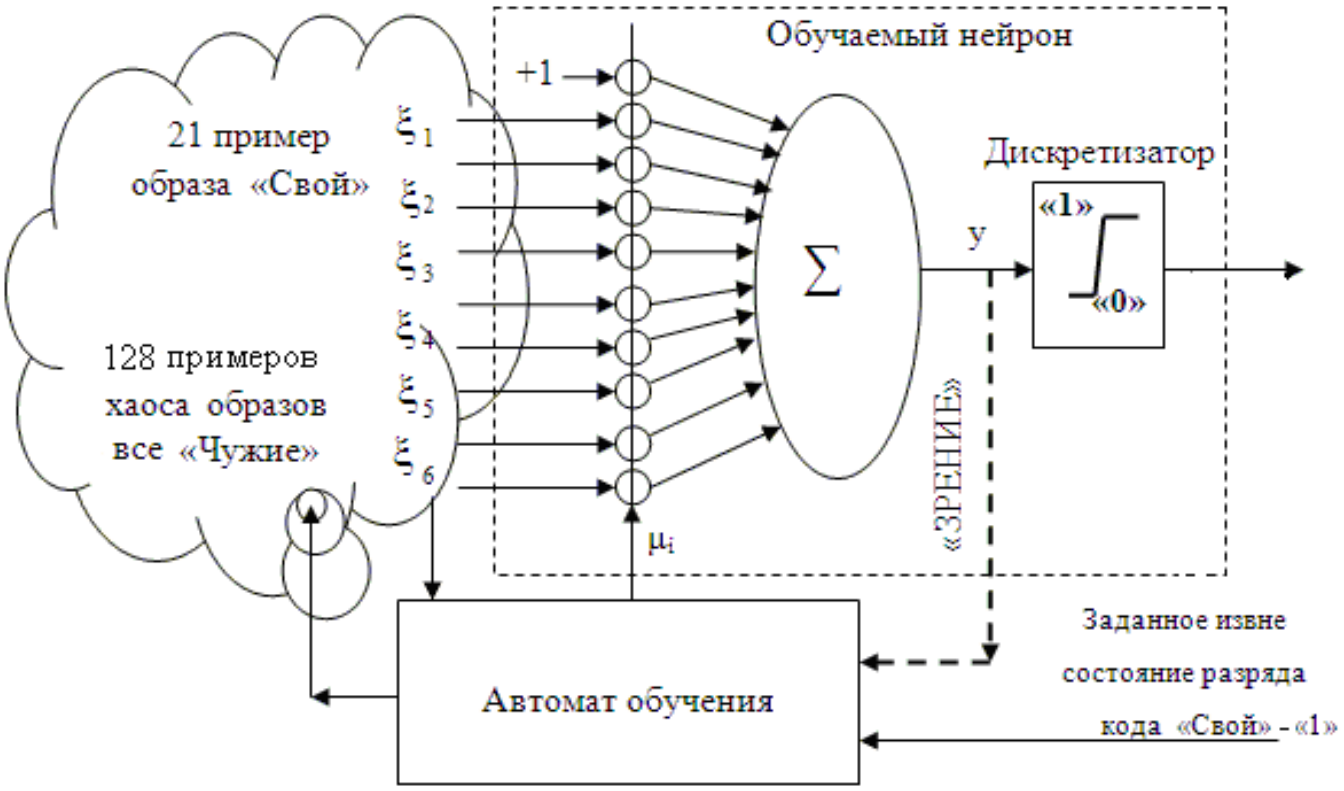


Рис. 4 Автоматическое обучение нейрона с малым числом входов

При обучении персептрона нет смысла наблюдать его выходные дискретные состояния «0» и «1». Как показано на рисунке 4, обучающий автомат должен наблюдать выходной сигнал сумматора. Обычно процедура обучения строится на том, что на первой итерации выбирают единичные значения весовых коэффициентов. Если поступать так, то мы получим необученный нейрон с распределением значений «Свой» в центре распределения все «Чужие», как это показано в левой части рисунка 5.

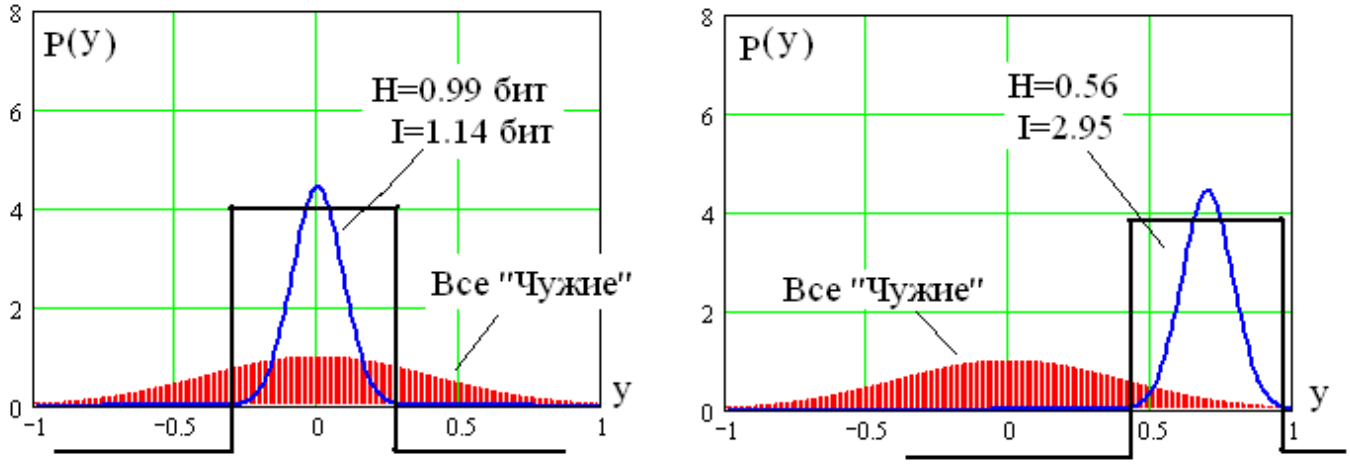


Рис. 5. Настройка нейрона за счет правильного выбора знаков весовых коэффициентов

Расположение в центре образов все «Чужие» распределения образа «Свой» невыгодно. Более выгодным является выталкивание распределения образа «Свой» на периферию распределения образов все «Чужие». Будем выталкивать распределение образов «Свой» в правую сторону. Для этого следует выбирать знаки при весовых коэффициентах следующим образом:

$$\begin{cases} \text{sign}(\mu_i) \to +(.) \quad \text{if } E(\xi_{i,\text{Свой}}) \geq E(\xi_{i,\text{Чужие}}); \\ \text{sign}(\mu_i) \to -(.) \quad \text{if } E(\xi_{i,\text{Свой}}) \langle E(\xi_{i,\text{Чужие}}). \end{cases} \qquad (8).$$

При таком выборе знаков происходит смещение распределения «Свой» в правую сторону, как это отображено в правой части рисунка 5.

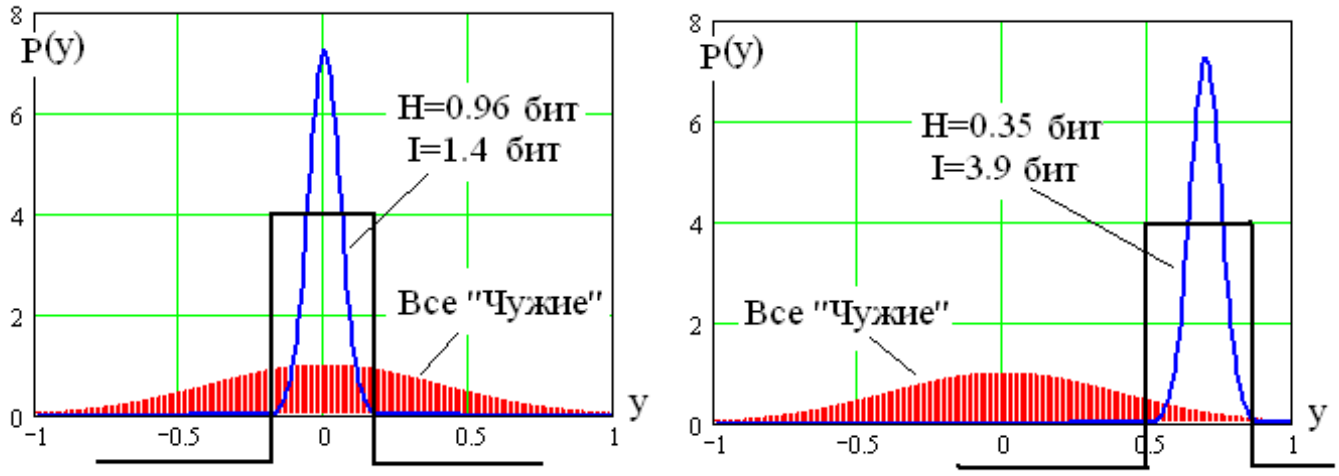


Рис. 6. Настойка нейрона за счет выбора значений весовых коэффициентов

Если случайно окажется, что все математические ожидания распределений параметров образов «Свой» нулевые $E(\xi_{i,Свой}) = 0$, то смещения в правую сторону не происходит (левая часть рисунка 6). В этом случае настройка нейрона может быть осуществлена только подбором значений весовых коэффициентов. Подбор осуществляется итерационно, при этом использовать энтропийный показатель качества обучения нельзя. Энтропия выходных состояний хорошо обученного нейрона оказывается много меньше энтропии необученного нейрона. При обучении следует использовать информационный показатель качества (5), из которого легко получить вероятность ошибки второго рода (ошибочного принятия «Чужого» за «Своего»):

$$P_2 = \frac{1}{2^{I(\xi_1)}} \qquad (9),$$

полагаясь на то, что вероятность ошибок первого рода нас устраивает и не меняется $P_1 \approx 0.01$. На рисунках 5 и 6 даны соответствующие значения энтропийного показателя и

информационного показателя качества обучения.

Обычно подбор весовых коэффициентов осуществляют вычисляя частную производную информационного показателя качества по каждому из подбираемых весовых коэффициентов. Если производная положительна, то весовой коэффициент увеличивают пропорционально ей:

$$\Delta\mu_i \approx \beta \cdot \frac{\partial I}{\partial \mu_i} \qquad (10),$$

где β- масштабный коэффициент.

При отрицательной частной производной осуществляют снижение того или иного весового коэффициента. В результате удается достаточно быстро найти оптимальные значения весовых коэффициентов нейрона или обучить его.

Следует подчеркнуть, что описанный выше способ обучения, как правило, инвариантен к виду пороговых нелинейностей на выходе нейрона. Обычно происходит одновременное сжатие распределения откликов образа «Свой» и его выталкивание из центра распределения откликов все «Чужие», как это показано в правой части рисунка 6. В этой ситуации четную и нечетную нелинейные пороговые функции можно замещать без особого ущерба для качества принимаемых нейроном решений.

6. Абсолютно устойчивые не итерационные алгоритмы обучения нейрона с неограниченным числом входов

К сожалению, итерационные алгоритмы обучения нейронов не способны обучать нейроны с большим числом входов. Это

обусловлено наступлением «слепоты» обучающего автомата, оказывающегося неспособным «увидеть» влияние одного из 1000 входов нейрона на конечный результат обучения. Чем больше входов у нейрона, тем меньше влияние каждого из этих входов на его выход. С ростом числа входов утрачивается линейная связь приращения весового коэффициента с его частной производной (10). Появляются так называемые «ложные» локальные максимумы качества, примеры которых даны на рисунке 7.

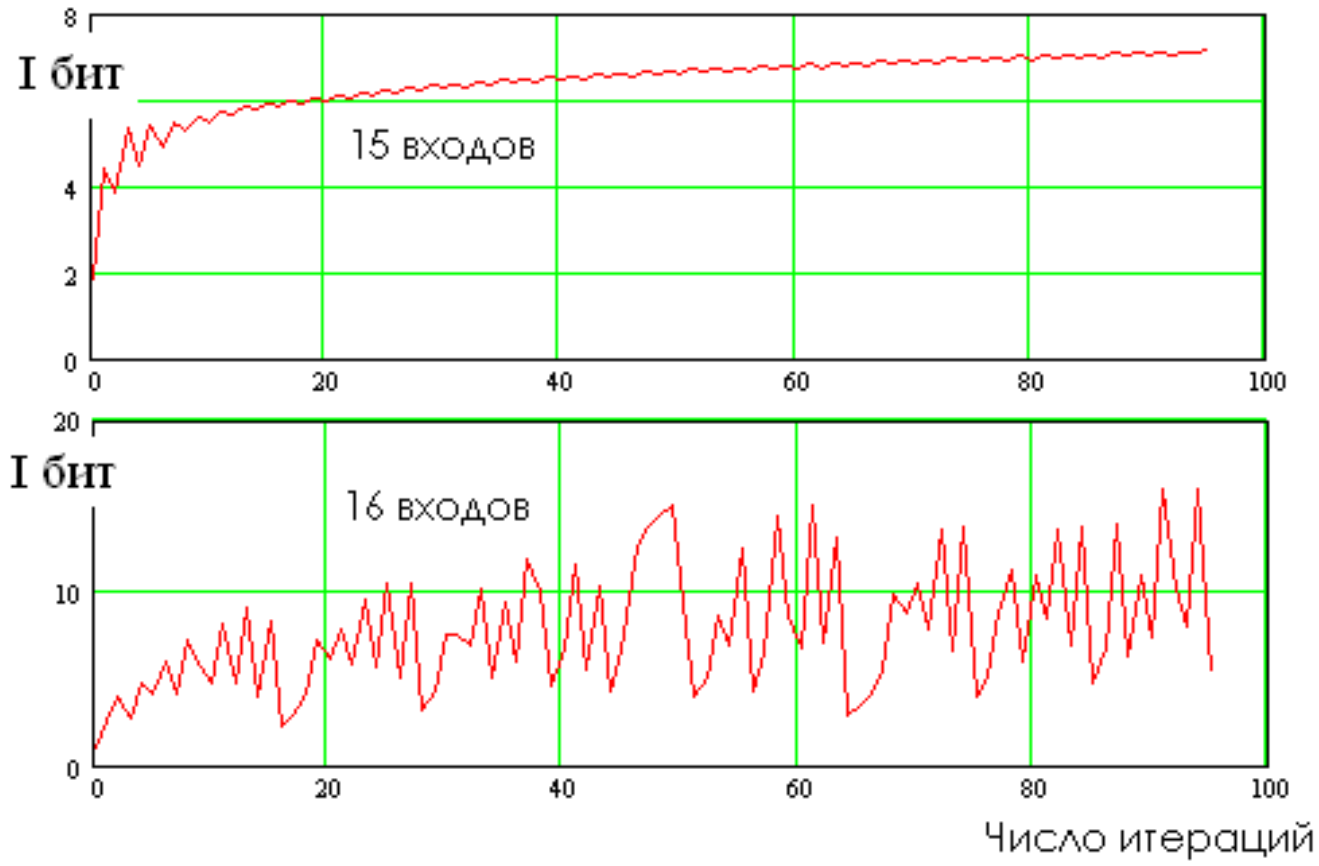


Рис. 7. Потеря устойчивости итерационного автомата обучения искусственного нейрона при увеличении числа входов

Из рисунка 7 видно, что при 15 входах у обучаемого нейрона на траектории повышения качества обучения (верхняя часть рисунка 7) практически нет ложных максимумов качества. Однако как только мы увеличиваем число входов у обучаемого нейрона до

16 (нижняя часть рисунка 7) ситуация кардинально меняется. Появляется огромное количество ложных максимумов качества, итерационный поиск глобального максимума качества теряет устойчивость. Все это можно рассматривать как ситуацию, когда обучение стало некорректным из-за недостаточности обучающей выборки примеров «Свой» для соответствующего числа обусловленности процедуры итерационного обучения нейрона с 16 входами.

Подчеркнем, что в случае обнаружения неустойчивости процедур итерационного обучения сделать их устойчивыми можно двумя способами. Нужно либо снизить число обусловленности процедуры обучения, например, снизив число входов у нейрона, либо следует снизить ошибку представления входных данных, например, увеличив число примеров «Свой», используемых при обучении. В обоих случаях ложные локальные максимумы качества обучения исчезают.

Для нас важно то, что нейроны в нейросетевых преобразователях биометрия-код одновременно осуществляют как обогащение входных биометрических данных, так и их дискретизацию. При этом, чем «хуже» входные данные, тем сильнее их следует обогащать перед дискретизацией. Нейроны, работающие с «плохими» биометрическими данными, должны иметь большее число входов. При этом, потеря устойчивости обучения для «плохих» данных наступает быстрее. Эта ситуация отображена на рисунке 8.

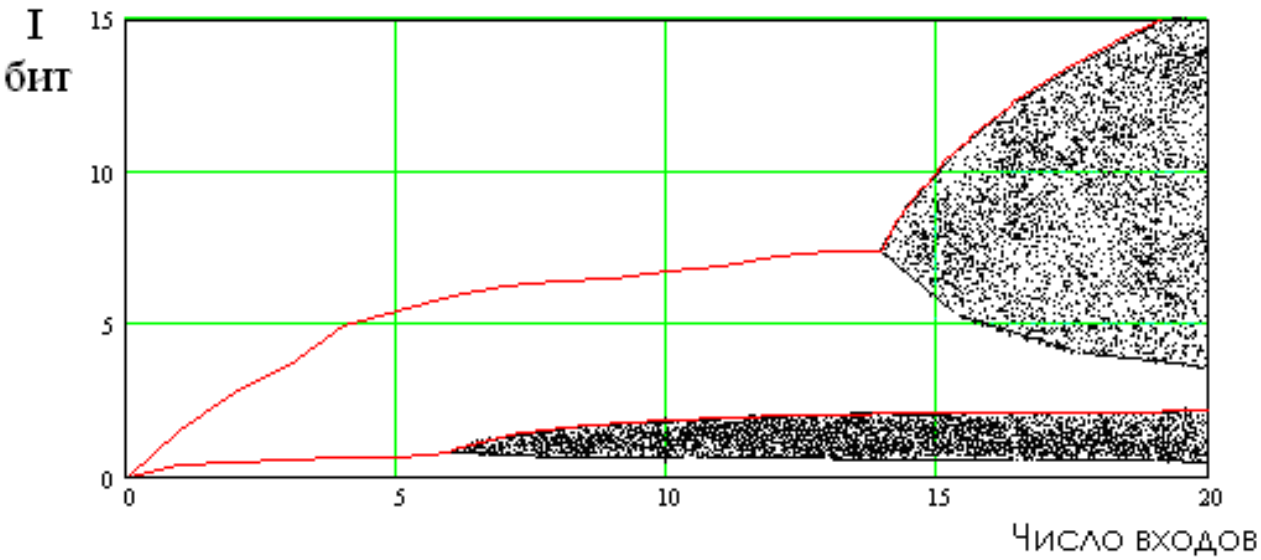


Рис.8. Потеря устойчивости обучения для данных «плохого» качества происходит при 7 входах у нейрона, тогда как для «хороших» данных срыв устойчивости происходит при 15 входах

Данные, отображенные на рисунке 8, соответствуют ситуации, когда автомат итерационного обучения был настроен на выполнения заданного числа итераций (96 итераций см. рисунок 7). Пока число входов у обучаемого нейрона мало, результаты обучения хорошо повторяются так как они находятся на монотонной поверхности оптимизации. При потере устойчивости обучения результат 96 итераций оказывается непредсказуемым, так как автомат обучения начинает блуждать по сильно изрезанной многомерной поверхности оптимизации критерия (10).

На рисунке 8 хорошо видны точки бифуркации процесса обучения (точки потери устойчивости итерационного обучения). При «плохих» входных данных качество обучения нейрона (10) оказывается низким и срыв устойчивого (монотонного) роста качества происходит при меньшем числе входов у нейрона. При «хороших» входных данных кривая качество обучения теряет устойчивость позднее (при большем числе входов у нейрона),

однако, потеря устойчивости процесса итерационного обучения все равно происходит, если мы пытаемся увеличивать размерность итерационно решаемой задачи. На рисунке 8 области неустойчивого поведения автомата обучения (слепоты автомата обучения) помечены темной заливкой. В связи с попаданием автомата обучения в неустойчивый режим разработчики стандарта ГОСТ Р 52633.5-2011 [7] вынуждены были отказаться от применения итерационных автоматов обучения нейронов.

По требования ГОСТ Р 52633.5-2011 [7] расчет весовых коэффициентов осуществляется по следующей формуле:

$$\mu_i = -\frac{E(\xi_{i,Чужие}) - E(\xi_{i,Свой})}{\sigma(\xi_{i,Чужие}) \cdot \sigma(\xi_{i,Свой})} \qquad (11).$$

Для того, чтобы вычислить любой их весовых коэффициентов нейрона, нет необходимости наблюдать отклик сумматора (на рисунке 4 обратная петля «ЗРЕНИЯ» обучающего автомата обозначена пунктирной линией связи). При обучении нейрона исчезает петля обратной связи и, соответственно, процедуры обучения оказываются абсолютно устойчивыми. То есть, мы имеем возможность обучать нейроны с любым числом входов. Видимо человек при обучении своих естественных нейронов головного мозга, имеющих порядка 10 000 входов, пользуется примерно таким же алгоритмом обучения.

7. Оценка качества нейросетевых решений на малых тестовых выборках

В случае, если мы отказываемся от неустойчивых

итерационных алгоритмов обучения нейронов (нейронных сетей), удается получить вероятности ошибок второго рода при учете нескольких сотен параметров на уровне $P_2 \approx 0.000000001$ и менее, что эквивалентно значению информационного показателя качества $I \approx 30$ бит. Казалось бы, что для подтверждения столь высоких показателей качества потребуются очень большие тестовые выборки, однако это далеко не так. Если мы продолжаем оставаться на линейном выходе сумматора нейрона, то в этой точке хорошо работает основная теорема статистики о нормализации большого числа данных [9, 10]. То есть, на выходе «обученного» сумматора с несколькими сотнями входов распределение значений все «Чужие» и распределение значений «Свой» будут описываться нормальными законами, как это отображено на рисунке 9.

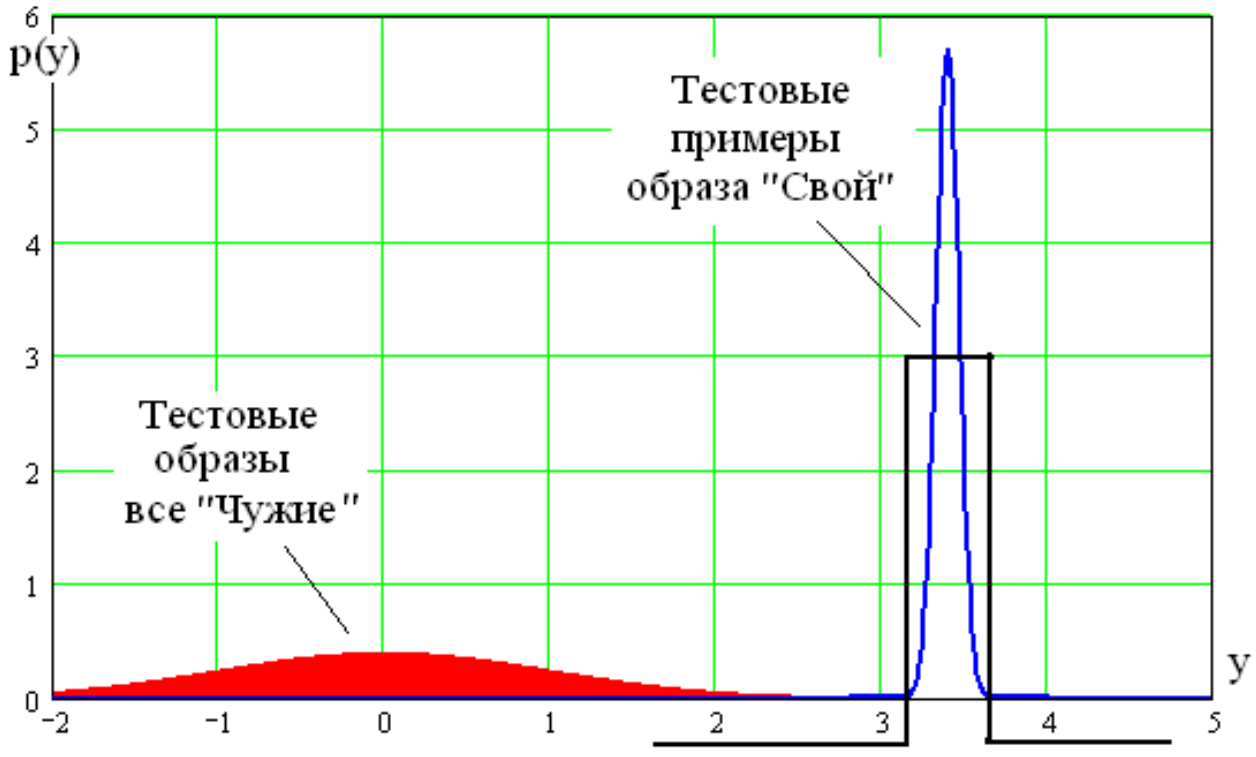


Рис. 9. Значения плотностей распределения для тестовых выборок образов «Чужие» и примеров «Свой» на выходе сумматора обученного нейрона

Факт того, что мы имеем дело с линейной обработкой данных и нормальными законами распределения значений, позволяет упростить задачу тестирования. Для тестирования качества могут быть использованы малые тестовые выборки примеров «Свой», не участвовавшие в обучении, и образов «Чужие», так же не участвовавшие в обучении нейрона. Для надежной оценки «нано» и «пико» вероятностей ошибок второго рода достаточно порядка 100 образов «Чужие» и 100 примеров образа «Свой». По тестовой выборке из 100 чисел мы способны вычислить математические ожидания $E(y_{Свой})$ и $E(y_{Чужие})$ и среднеквадратические отклонения $\sigma(y_{Свой})$ и $\sigma(y_{Чужие})$. Зная эти параметры, мы можем рассчитать вероятность появления ошибок второго рода:

$$P_2 = \frac{1}{\sigma(y_{Чужие})\sqrt{2\pi}} \int_a^b \exp\left(\frac{-u^2}{2 \cdot \sigma^2(y_{Чужие})}\right) \cdot du \qquad (12),$$

где $a = E(y_{Свой}) - 3 \cdot \sigma(y_{Свой})$;

$b = E(y_{Свой}) + 3 \cdot \sigma(y_{Свой})$.

Таким образом, рассматриваемое нейросетевое решение имеет не только алгоритм быстрого не итерационного обучения, но и алгоритм быстрого тестирования на малых обучающих выборках.

8. Сети нейронов с внутренней кодовой избыточностью

Следует отметить, что короткий алфавит, состоящий только из двух состояний «1» и «0» («Свой» или «Чужой») является частным случаем более длинных алфавитов, например, рукописный алфавит русского языка состоит из 33 букв, причем написание

заглавных и прописных букв разное. То есть, если мы будем создавать индивидуальный нейросетевой искусственный интеллект, способный самообучаться и распознавать рукописный почерк своего хозяина, то нам придется использовать нейросеть примерно с 80 выходами. Тогда каждый выход должен давать состояние «1» при распознавании своего рукописного знака (рукописной буквы или цифры), а все другие выходы должны давать состояние «0».

При анализе динамики рукописного воспроизведения одиночных знаков нельзя получать неограниченное число параметров. Практика показала, что анализируя кривые x(t) и y(t) движения пера при воспроизведении буквы удается использовать не более 200 параметров. Из-за относительной простоты одиночной буквы извлекать 1000 параметров бессмысленно, 1000 контролируемых параметров эффективна только при анализе рукописного пароля из 5 букв.

Если мы для всех 200 анализируемых параметров обучим нейрон на выделение рукописной буквы «*а*» по алгоритму, описанному в параграфе 6, то на выходе сумматора нейрона мы получим достаточно далеко вытолкнутое из распределения «Чужие» распределение откликов «*а*» (рисунок 10). При этом, распределения всех иных рукописных букв будут достаточно сильно перекрываться (оказываются слабо разделимыми).

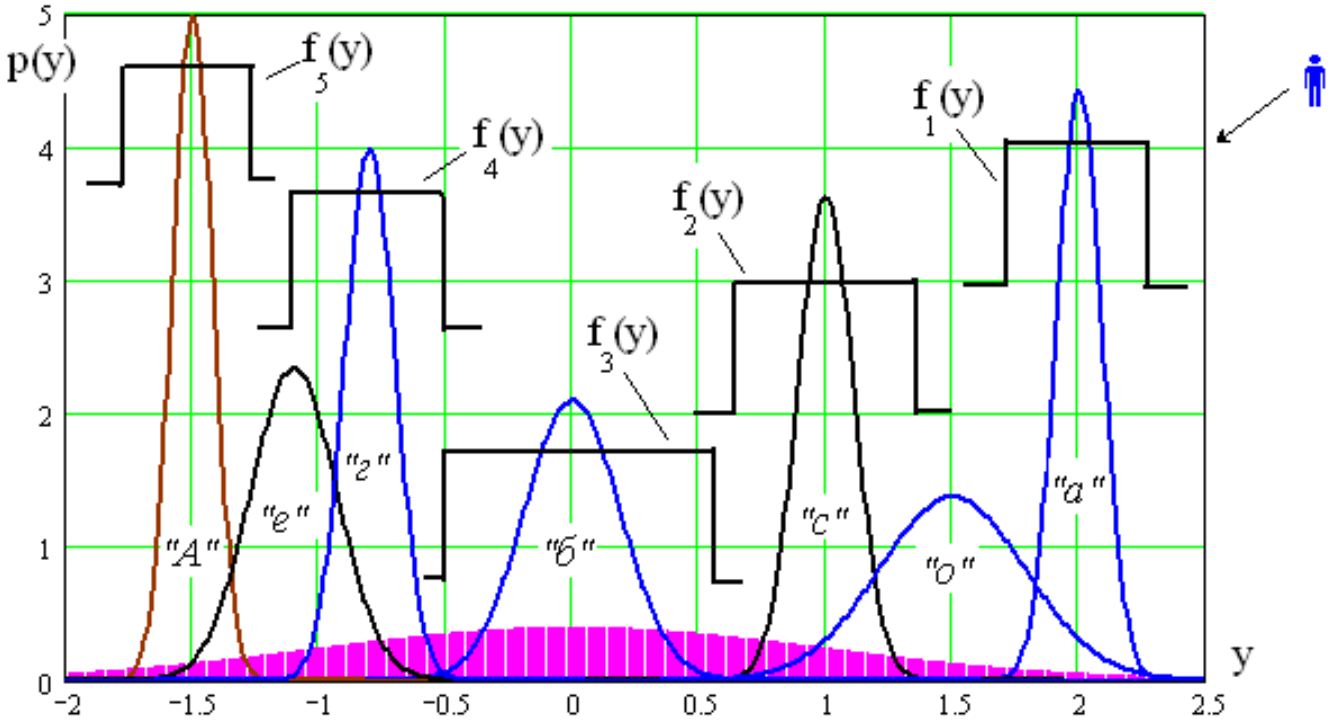


Рис. 10. Пример распределений откликов разных рукописных букв на выходе сумматора нейрона, обученного распознавать рукописный символ «*а*»

Как видно из рисунка 10 рукописный символ «*а*» достаточно хорошо отделяется от данных все «другие знаки», однако, он неотделим от своих ближайших соседей. В связи с этим, нейронами первого слоя необходимо выделять только достаточно компактные множества. Каждое из компактных множеств должно выделяться своей нелинейной функцией $f_1(y)$, $f_2(y)$, …., $f_n(y)$, как это показано на рисунке 10. В конечном итоге мы имеем нейрон первого слоя с несколькими выходами, его структура отображена на рисунке 11.

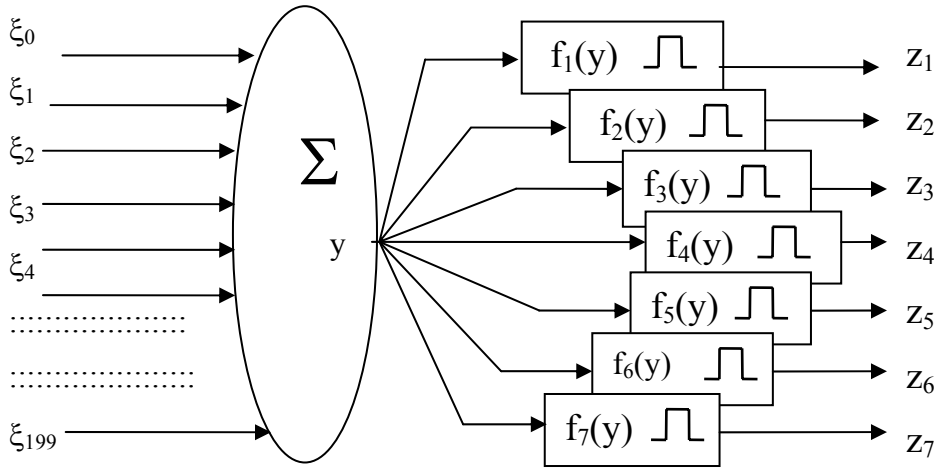


Рис. 11 Искусственный нейрон с несколькими выходами

Первый слой нейросети должен иметь число нейронов, совпадающее с числом распознаваемых классов (в нашем случае 80), каждый сумматор каждого нейрона должен быть обучен на распознавание своего знака с распределением, сдвинутым как можно правее от центра множества все «знаки». Операция обучения нейронов первого слоя может интерпретироваться как вращение 200-мерной сферы с целью подбора наиболее удобной точки наблюдения за распределением конкретных знаков. Эта операция иллюстрируется рисунком 12 на примере всего лишь 2-х мерной сферы.

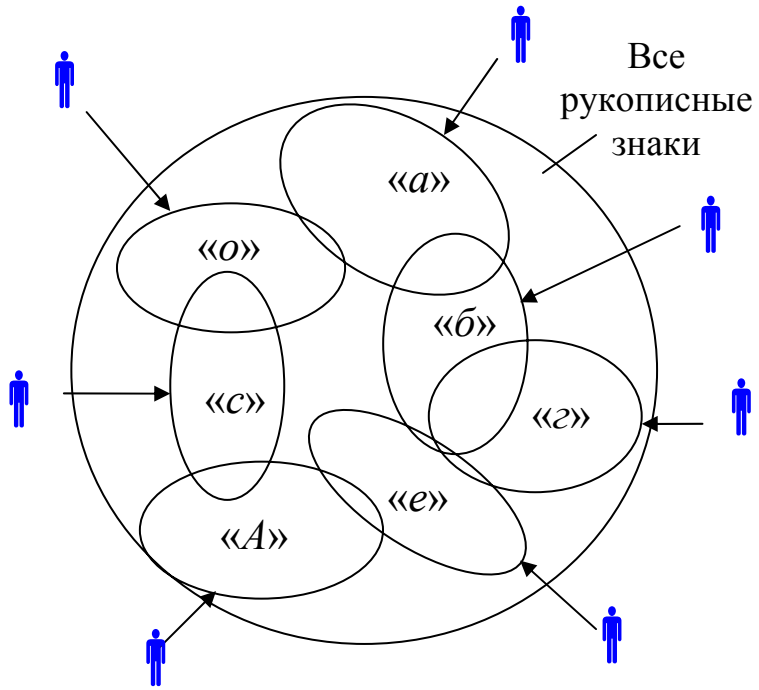


Рис. 12. Иллюстрация подбора наиболее удобного ракурса наблюдения того или иного распределения параметров на выходе «обучаемого» сумматора

Если мы у каждого из нейронов первого слоя обеспечим только 16 выходов, то получим коды с 15-ти кратной избыточностью. Имея столь существенную избыточность кодов можно воспользоваться классической теорией самокорректирующихся избыточных кодов [11] и создать автомат, обнаруживающий и исправляющий ошибки распознавания. Однако, путь использования классических самокорректирующихся кодов [11] нерационален. Классические коды строятся исходя из гипотезы равновероятного распределения ошибок, а в биометрии (при распознавании рукописных символов) эта гипотеза не работает.

Гораздо более эффективным способом коррекции ошибок кодов первого слоя является использование нейронов второго слоя и обучения их по одной из модификаций алгоритма, изложенного в разделе 7 ГОСТ Р 52633.5-2011 [7]. Обучение

должно вестись с учетом реально наблюдаемых вероятностей ошибок в каждом разряде биометрических кодов первого слоя нейронной сети.

В самом простом варианте на входах нейронов второго слоя достаточно собрать все отклики нейронов первого слоя с нелинейными элементами, выделяющими один и тот же символ. Весовой коэффициент по каждому входу нейрона второго слоя выбирается пропорционально коэффициенту стабильности появления состояний «1» на входе нейрона при предъявлении нейронной сети обучаемого символа. При высокой стабильности весовой коэффициент связи оказывается единичным. При низкой стабильности весовой коэффициент может оказаться нулевым. Решение о выявлении того или иного символа принимается по наибольшему значению на выходах нейронов второго слоя.

9. Линейная алгебра: сети квадратичных форм

Линейная алгебра [12, 13] является очень удобным математическим аппаратом для уяснения сути алгоритмов и их потенциальных возможностей. В частности, крайне интересным является использование для распознавания образов n-мерных квадратичных форм:

$$y_n = \sqrt{(\overline{\xi} - E(\overline{\xi}))^T \cdot [\rho_{ij}]^{-1} \cdot (\overline{\xi} - E(\overline{\xi}))} \qquad (13),$$

где $[\rho_{ij}]^{-1}$- обратная n-мерная матрица коэффициентов ковариации; каждый из коэффициентов ковариации -ρ_{ij} в матрице вычисляется по следующей формуле:

$$\rho_{ij} = \frac{1}{N}\sum_{m=1}^{N}(\xi_{im} - E(\xi_{im})) \cdot (\xi_{jm} - E(\xi_{jm})) \qquad (14),$$

где N – число примеров образа «Свой», использованных при расчете коэффициентов ковариации.

Квадратичные формы всегда положительны и показывают расстояние по радиусу n-мерного эллипса в n-мерном пространстве. Настройка (обучение) распознаванию образа «Свой» в n-мерном пространстве сводится к вычислению n-мерной ковариационной матрицы по N примерам образа «Свой», обращения этой ковариационной матрицы и определению максимального значения показания расстояний квадратичной формы для примеров образа «Свой» - $\max(y_n)$.

По значению порога - $\max(y_n)$ квадратичная форма легко дискретизируется. Если ее отклик меньше значения $\max(y_n)$, то возникает состояние «1» и предъявленный n-мерный образ воспринимается как «Свой». Если значение квадратичной формы оказывается более чем $\max(y_n)$, то ему присваивается состояние «0», предъявленный n-мерный образ рассматривается как «Чужой». Эта окончательная настройка иллюстрируется рисунком 13.

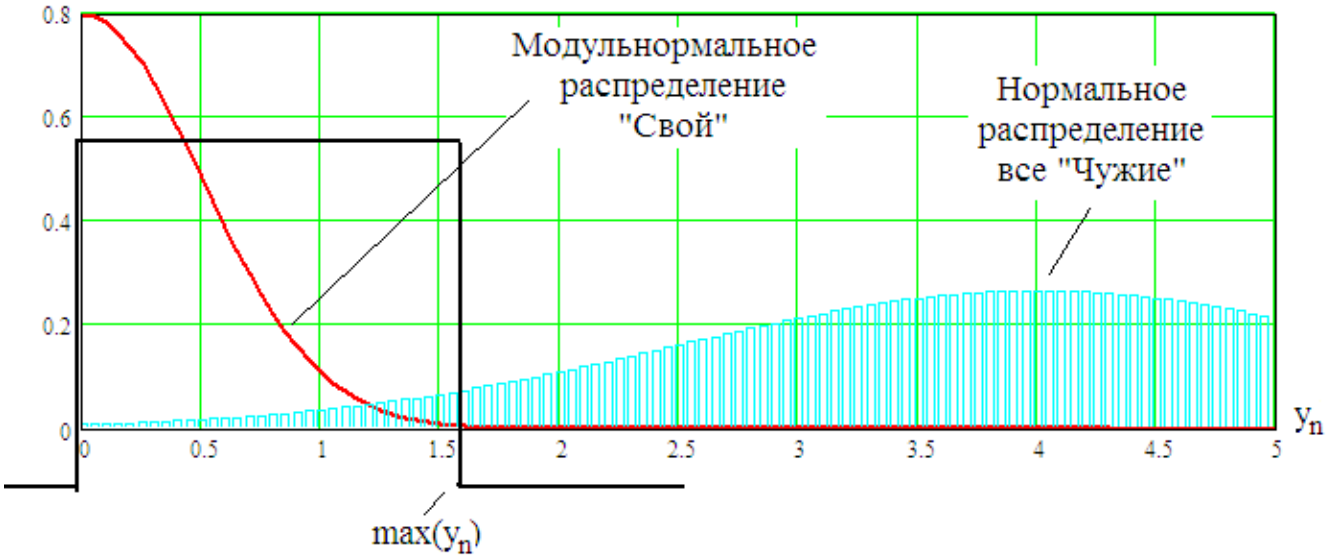


Рис. 13. Окончательная настройка квадратичной формы путем выбора порога разграничения образов «Свой» и «Чужие»

Так как в процедуру настройки (обучения) квадратичных форм входит операция обращения матриц возникает проблема устойчивости вычислений. Повышать устойчивость обращения ковариационной матрицы можно по Тихонову или за счет привлечения избыточных данных, однако, эти приемы регуляризации не дают кардинального решения задачи. Трудно себе представить то, что кому то удастся эффективно обращать хотя бы 100-мерные ковариационные матрицы, а вот 10-мерные ковариационные матрицы технически обратимы. Получается, что простое использование классической квадратичной формы (8) не способно давать высоко-размерные решения. Выход из этого тупика состоит в использовании сети квадратичных форм низкой размерности.

Например, если нам требуется анализировать совокупность из 1000 параметров, а обращать мы способны только 10-мерные ковариационные матрицы, то мы можем использовать сеть из 256 десятимерных квадратичных форм. При этом входные связи

каждой из квадратичных форм могут задаваться случайно. Тогда две случайно выбранные квадратичные формы будут иметь общие входные параметры с пренебрежимо малой вероятностью 0,01. Такая сеть квадратичных форм будет откликаться кодом из почти 256 единиц при предъявлении ей образа «Свой» и кодом из почти 256 нулей при предъявлении ей образа «Чужой».

Независимо от того, что мы предпочитаем использовать линейную алгебру с ее квадратичными формами или нелинейную алгебру нейросетевых функционалов; корректное решение высокоразмерных задач удается получить, только применяя множество простых устойчивых частных решений, объединенных в сеть. Сети квадратичных форм и сети из нейронов по своей сути мало чем отличаются от друг друга.

10. Нейросетевые эмуляторы квадратичных форм

Однако, классические квадратичные формы всетаки применять не следует из-за того, что они требуют вычисления обратных ковариационных матриц. Для биометрических данных легко вычислимы обратные ковариационные матрицы 2, 3, 4 порядков. Для более высоких размерностей задач приходится прибегать к специальным вычислительным приемам. Задача обращения матриц относится к не корректным (неустойчивым), однако ее можно решить, например, регуляризацией по Тихонову [14]. Можно пойти иным путем и улучшить устойчивость за счет использования большего числа исходных данных [15, 16], входящих в переопределенные (избыточные) матрицы. Оба эти направления улучшения стабильности вычислений

нельзя рассматривать как эффективные. И в том и в другом случае не удается корректно обращать матрицы 10-го порядка и выше.

Гораздо более эффективным является полный отказ от использования процедуры обращения ковариационных матриц и переход из линейной алгебры в нелинейную алгебру матриц нейросетевых функционалов. Например, это можно сделать, применяя нейросетевые эмуляторы n-мерных квадратичных форм. Чтобы создать такой эмулятор необходимо использовать полносвязанные n нейронов с n входами, при этом каждый из нейронов должен иметь четную нелинейную функцию с единичным откликом на образ «Свой». Все выходы нейронов должны быть объединены одним коньюнктором (рис. 14).

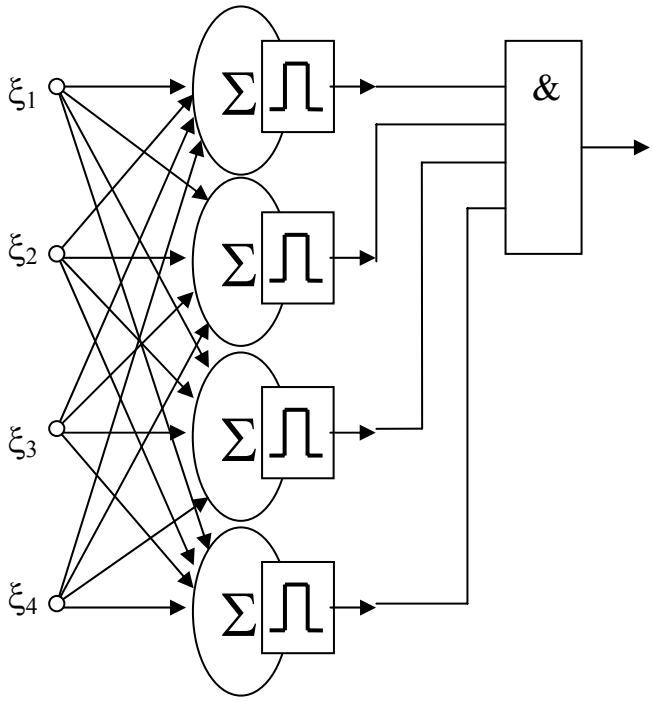


Рис. 14 Нейросетевой эмулятор четырехмерной квадратичной формы

Приведенная на рисунке 14 нейросетевая структура выдает состояние «1» при условии, если все четыре нейрона распознают предъявленный образ как «Свой». Каждый из искусственных

нейронов можно рассматривать как некоторого четырехмерного наблюдателя границ образа «Свой». На бумаге проиллюстрировать это удается только для двухмерного случая (рисунок 15).

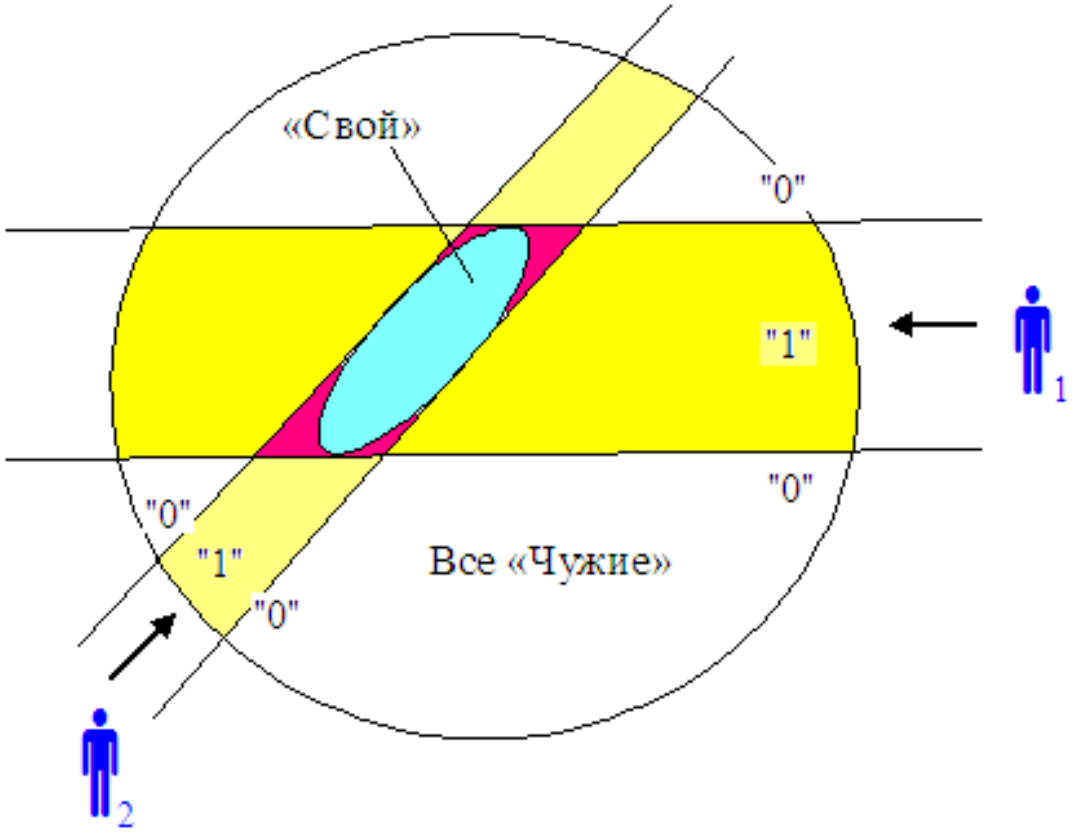


Рис. 15 Иллюстрация совместной работы двух наблюдателей (двух нейронов) в составе эмулятора квадратичной формы

Из рисунка 15 видно, что использование только одного нейросетевого наблюдателя позволяет в окружности все «Чужие» вырезать «коридор» возможных состояний. Два наблюдателя образуют два коридора наблюдения, которые описывают эллипс действительного распределения примеров образа «Свой» некоторым параллелограммом. Площадь параллелограмма и площадь вписанного в него эллипса оказываются близки, что и

является доказательством работоспособности нейросетевого эмулятора квадратичной формы. Можно показать, что с ростом размерности нейросетевого эмулятора относительная ошибка вычислений, возникающая из-за разницы гипперобъема гапперэллипса и описывающего его гиперпараллелепипеда, монотонно уменьшается. При этом нет необходимости добиваться взаимной ортогональности нейросетевых наблюдателей [17, 18], что существенно упрощает процедуры автоматического обучения нейросетевого эмулятора квадратичных форм. При обучении нейросетевого эмулятора квадратичных форм достаточно разнести в n-пространстве точки наблюдения каждого из нейронов. При этом число нейронов, образующих эмулятор квадратичной формы может не совпадать с размерностью решаемой ими задачи.

Принципиальным преимуществом нейросетевых эмуляторов квадратичных форм является то, что их легко удается реализовать как 32-мерными, так и более высокой размерности. По сравнению с классическими квадратичными формами линейной алгебры удается увеличить размерность решаемых задач в несколько раза.

Первый нейрон эмулятора квадратичной формы обучается максимизацией качества принимаемых им решений по ГОСТ Р 52633.5 [7]:

$$\max\left[Q_n = \frac{\left| E(y_{n,\text{Чужие}}) - E(y_{n,\text{Свой}}) \right|}{\sigma(y_{n,\text{Чужие}}) \cdot \sigma(y_{n,\text{Свой}})} \right] \qquad (15).$$

Последний нейрон необходимо обучать поиском максимума отношения среднеквадратических отклонений образов «Чужие» и «Свой»:

$$\max\left[q_n = \frac{\sigma(y_{n,\text{Чужие}})}{\sigma(y_{n,\text{Свой}})} \right] \qquad (16).$$

Так как показатели качества обучения Q_n и q_n определены различными способами (15) и (16), весовые коэффициенты первого и последнего нейронов μ_{1j} и μ_{nj} не совпадают. Для того, чтобы получить весовые коэффициенты всех остальных нейронов μ_{2j}, μ_{3j}, …, $\mu_{(n-1)j}$ n-мерного эмулятора квадратичной формы достаточно выбрать для них случайные значения, равномерно распределенные между j-ми весовыми коэффициентами первого и последнего нейронов.

11. Сети нейронов с высокой выходной кодовой избыточностью (нелинейная алгебра матриц высоко-размерных нейросетевых функционалов)

Одним из недостатков описанных выше нейросетевых решений является то, что заложенные в них при обучении знания легко извлекаются. Этот недостаток особенно неприятен при реализации биометрических технологий идентификации и аутентификации людей. На рисунке 16 дана иллюстрация одной из технологий извлечения знаний из обученной нейронной сети. Эта технология может быть условно названа атакой «поиска близнецов».

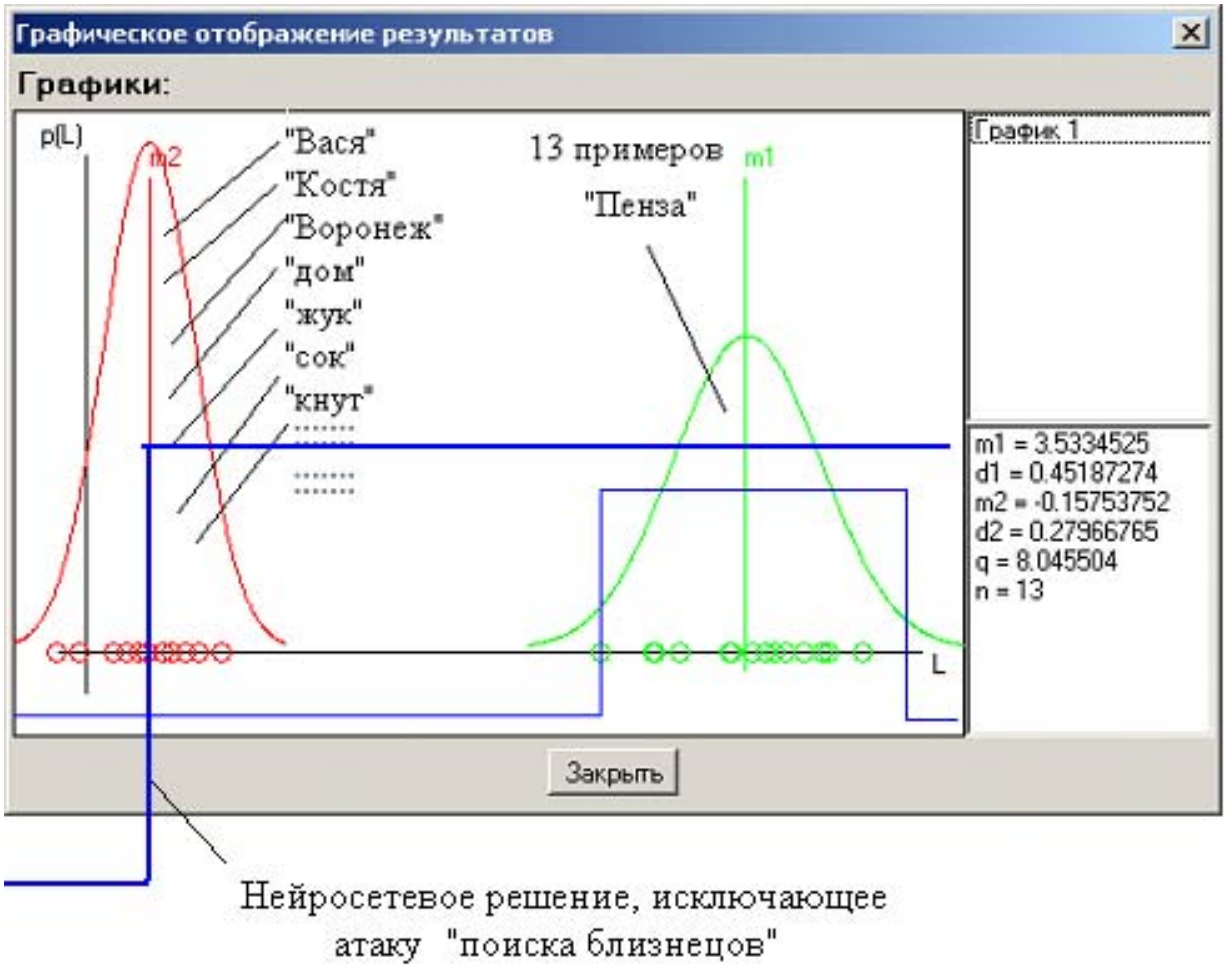


Рис. 16 Организация атаки «поиска близнецов» по базе биометрических образов (экранная форма взята из среды моделирования НейроПреподаватель 0.1, используемой для проведения лабораторных работ «Пензенским ГУ»)

Предполагается, что злоумышленник получил нейронную сеть, обученную распознавать биометрический образ человека «Свой». Нейронная сеть имеет один выход и дает состояние «1» при предъявлении ей образа «Свой». В этом случае для того, чтобы найти «близнеца» злоумышленнику нужно собрать большую базу биометрических образов и начать их предъявлять обученной нейронной сети. Если собранная база биометрических образов достаточно велика, то в ней найдется биометрический образ, который дает коллизию с образом «Свой» или является его близнецом. Именно по этой причине формирование больших баз

биометрических образов людей следует рассматривать как подготовку к атаке на биометрическую защиту.

Для того, чтобы исключить атаку поиска близнецов необходимо изъять знание о том, какое состояние выходного кода соответствует образу «Свой». То есть необходимо чтобы нелинейная функция на выходе у нейрона переключалась из одного состояния в другое в точке математического ожидания все «Чужие». При атаке «поиска близнецов» состояния «0» и состояние «1» решающего правила должны быть равновероятны. Кроме того, решающее правило не должно иметь последний бит или малое число последних бит. Должна быть ситуация, когда злоумышленник не может найти «последний» бит решающего правила и подменить его.

То есть, скрыть знания, размещенные в обученной нейронной сети, удается если нейронная сеть будет преобразовывать «тайный» биометрический образ человека в его «тайный» длинный код доступа (личный ключ). Тогда атака «поиска близнецов» не может быть удачной из-за того, что злоумышленник не знает код доступа. Подобрать этот код доступа злоумышленник так же не может из-за его большой длины. Восстановить код доступа злоумышленник не может из-за того, что не знает «тайный» биометрический образ «Свой».

Только в этом случае атака «поиска близнецов» в базе биометрических образов и атака поиска последнего бита в программе защиты становятся не эффективными. При этом, каждый из выходов нейронной сети должен плохо работать по отношению к образам «Чужой» и давать высокую вероятность

ошибок второго рода P_2 =0.5. А «Своего» каждый выход нейронной сети должен узнавать очень хорошо, обеспечивая низкий уровень вероятностей ошибок первого рода $P_1 \approx 0.01$.

Получается, что каждый из выходов нейронной сети с длинным выходным кодом работает очень плохо, однако, все вместе они работают очень хорошо, если обеспечена независимость (некоррелированность) выходов нейросети при атаке подбора случайными биометрическими образами «Чужие». Если предположить, что нейросетевой преобразователь биометрия-код имеет 256 выходов (число выходов совпадает с длиной ключа отечественных стандартов по шифрованию и формированию цифровой подписи), то уровень ошибок второго рода становится пренебрежительно мал. Для полностью независимых (некоррелированных) выходов обученной нейронной сети получаем:

$$P_2 \approx \frac{1}{2^{256}} \approx \frac{1}{10^{77}} \qquad (17).$$

Это фантастически малая величина практически никогда не встречающихся событий. Однако, оценка (17) является слишком оптимистичной. На практике полностью устранить корреляционные связи на выходах обученной нейронной сети не удается. По этой причине базовый национальный стандарт ГОСТ Р 52633.0-2006 [19] допускает у обученного преобразователя биометрия-код наличия небольших парных корреляционных связей его выходов. Допускается наличие парных корреляционных связей, среднее значения модуля которых не превышает 0.15. В предельном случае, когда $E(|r|)=0.15$, значения показателей в оценке (17)

уменьшаются примерно в 10 раз:

$$P_2 \approx \frac{1}{2^{25.6}} \approx \frac{1}{10^{7.7}} \qquad (17а).$$

Принципиальным отличием решением задачи высоконадежной биометрической аутентификации личности от задачи распознавания рукописного почерка является то, что при обучении нейронной сети должна сохраняться тайна личного ключа пользователя и тайна его биометрического образа (рукописного или голосового пароля). То есть обучение нейронной сети должен обязательно выполнять автомат, а данные, использованные для обучения, должны быть удалены. Наличие автомата обучения обязательно, так как появление посторонних людей при обучении недопустимо, из-за возникновения угрозы компрометации конфиденциальности данных обучения. Обобщенная блок-схема процедуры автоматического обучения отображена на рисунке 17.

Обучающий автомат следует реализовывать по стандарту ГОСТ Р 52633.5-2011 [7], применяя однослойную или двухслойную сеть нейронов. При обучении добиваются смещения распределения откликов сумматора нейрона на образы «Свой» в правую сторону, если выход нейрона отвечает за разряд кода ключа с состоянием «1» (см. рисунок 17). Если выход нейрона отвечает за разряд кода ключа с состоянием «0», то распределение откликов на примеры образа «Свой» смещают в левую сторону от центра распределения образов все «Чужие».

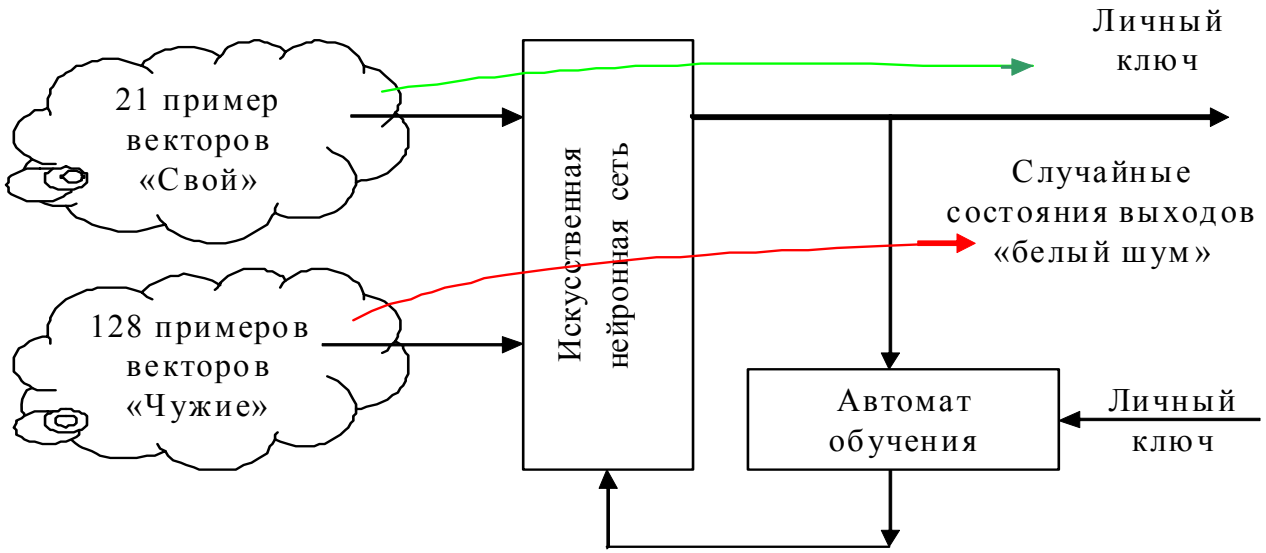


Рис. 17 Общая схема процедуры обучения нейросетевого преобразователя биометрия-код

Автоматическое обучение нейронной сети преобразователя биометрия-код осуществляется очень быстро, так как каждый из нейронов обучается независимо и без осуществления итерационного поиска глобального максимума качества обучения. Двухслойная нейросеть с 256 нейронами в первом и втором слое (каждый нейрон имеет по 32 входа) обучается за время менее 1 секунды, при использовании обычной ПЭВМ.

Получающийся после обучения нейросетевой преобразователь биометрия-код (НПБК) при воздействии на него примерами образа «Свой» и образа «Чужой» ведет себя совершенно по разному. При воздействии образами «Свой» НПБК устраняет естественную энтропию образов «Свой» и дает однозначный выходной код - $\overline{c}$:

$$\left[\begin{matrix}\text{НПБК}\\ N\times n\end{matrix}\right]\cdot\overline{\xi}_i=\overline{c} \qquad (18),$$

где $\overline{\xi}_i$ - вектор из N входных биометрических параметров, полученных из i-го примера образа «Свой»;

$\overline{c}$ - бинарный код из n разрядов (вектор из n бинарных состояний каждого из разрядов кода), соответствующий отклику НПБК на образ «Свой»;

$\begin{bmatrix} \text{НПБК} \\ N \times n \end{bmatrix}$ - матрица нелинейных нейросетевых функционалов, дискретизирующих (преобразующих) вектор входных непрерывных биометрических данных в выходной код.

При воздействии примерами образа «Чужой» НПБК усиливает естественную энтропию образов «Чужой» и дает псевдослучайные выходные коды - $\overline{x}_i$:

$$\begin{bmatrix} \text{НПБК} \\ N \times n \end{bmatrix} \cdot \overline{\xi}_i = \overline{x}_i \qquad (19),$$

где $\overline{\xi}_i$ - вектор из N входных биометрических параметров, полученных из i-го примера образа «Чужой»;

$\overline{x}_i$ - бинарный код длиной n бит, соответствующий разным откликам НПБК на разные примеры образа «Чужой».

Энтропия псевдослучайных выходных кодов $\overline{x}_i$ всегда оказывается существенно меньше своего максимально возможного значения:

$$H(\overline{x}) = H(x_1, x_2, ..., x_n) \langle n \text{ бит} \qquad (20).$$

Для того, чтобы сделать энтропию выходных кодов максимально возможной необходимо осуществить самошифрование данных обученной нейронной сети [20, 21] на

части выходного ключа $\overline{c}$. Самошифрование осуществляется сложением по модулю два - $\oplus$ части разрядов ключа $\overline{c}$ с адресами связей нейронов и весовыми коэффициентами, обученной нейронной сети. Так как для всех примеров образа «Свой» НПБК дает один и тот же код, то возможно не только самошифрование данных нейросети после ее обучения, но и их саморасшифрование во время процедуры аутентификации. Обе эти ситуации отображены на рисунке 18.

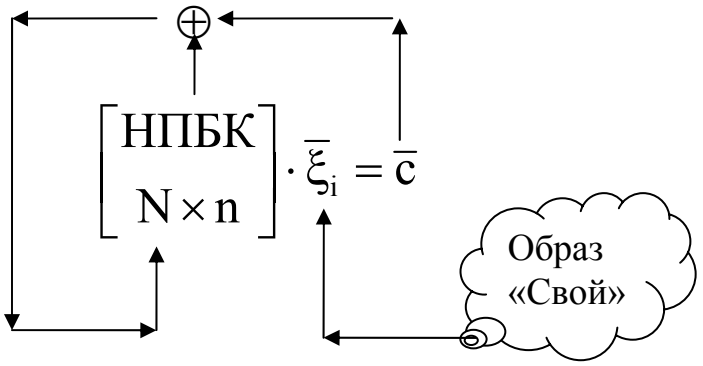


Рис. 18. Самошифрование и саморасшифрование НПБК при работе с данными «Свой»

Совершенно иная ситуация возникает, когда расшифровать защищенный самошифрованием НПБК пытается «Чужой». Данные «Чужого» дают псевдослучайный выходной код - $\overline{x}_i$, не совпадающий с кодом самошифрования - $\overline{c}$. То есть саморасшифровывания данных обученного НПБК не происходит. Возникает эффект размножения ошибок, который приводит к хешированию (перемешиванию) выходных кодов НПБК. При этом остаточные корреляционные связи, присутствующие между разрядами кодов $\overline{x}_i$, исчезают. Блок-схема самохеширования

кодов «Чужой» приведена на рисунке 19.

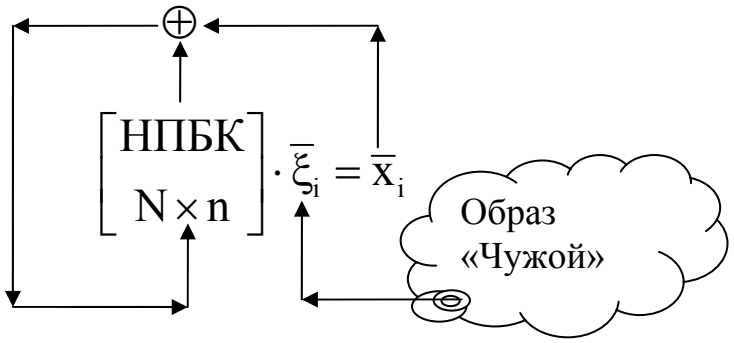


Рис. 19. Самохеширование кодов «Чужой» при попытках расшифровать на случайном ключе ранее защищенный самошифрованием на ключе $\overline{c}$ НПБК

В силу хеширование данных по схеме рисунке 19 их энтропия становится максимально возможной, неравенство 20 становится тождеством.

12. Генетический алгоритм обращения матриц нейросетевых функционалов

Получается, что на уровне подсознания (естественного или искусственного) происходит связывание образов высоко-размерной непрерывной действительности с кодами-словами некоторого языка гораздо более низкой размерности. Фактически, ГОСТ Р 52633.5-2011 [7] – это описание одного такого пути нейросетевого связывания конечного множества континуумов непрерывных данных с некоторым конечным множеством дискретных кодо-слов языка общения. Возникает вопрос, осуществимо ли обратное преобразование для матриц нейросетевых функционалов? Можно ли, зная выходное слово-код и имея обученный НПБК, восстановить

соответствующий входной вектор биометрических параметров образа «Свой»?

Эта задача является далеко не праздной. Действительно, эффективная система кодирования должна иметь как прямое, так и обратное преобразование. Только обладая прямым и обратным преобразованием можно получить действительно надежные средства распознавания образов, ошибки которых могут быть достоверно оценены. Обратное преобразование или обращение матриц нейросетевых функционалов описывается стандартом ГОСТ Р 52633.3-2011 [10]. Суть стандарта сводится к тому, что при тестировании заранее должна быть сформирована достаточно большая база естественных биометрических образов «Чужие», в которой образа «Свой» может и не оказаться. Размеры тестовой базы и то, как она собирается описаны в стандарте ГОСТ Р 52633.1-2009 [22]. Имея достаточно большую базу тестовых биометрических образов, мы получаем возможность предъявлять их НПБК в произвольном порядке. При этом, каждый предъявленный биометрический образ даст на выходе НПБК свое кодовое слово «Чужой-i». Тестируя НПБК, мы можем получить несколько сотен кодовых слов «Чужой-1», «Чужой-2», …., «Чужой-1024».

Последующие статистические расчеты необходимо осуществлять в пространстве расстояний Хэмминга между кодом образа «Свой» и всеми иными кодами образов «Чужой-i»:

$$h_i = \sum_{k=1}^{n} (c_k \oplus x_{k,i}), \qquad (21)$$

где c_k – значение k-го разряд кода «Свой»; $x_{k,i}$. – значение k-го

разряда кода i-го образа «Чужой-i».

Из теории известно, что для кодов длинной более 32 бит распределение расстояний Хэмминга хорошо описывается нормальным законом распределения значений. На рисунке 20 приведены примеры таких распределений для кодов длинной 256 бит.

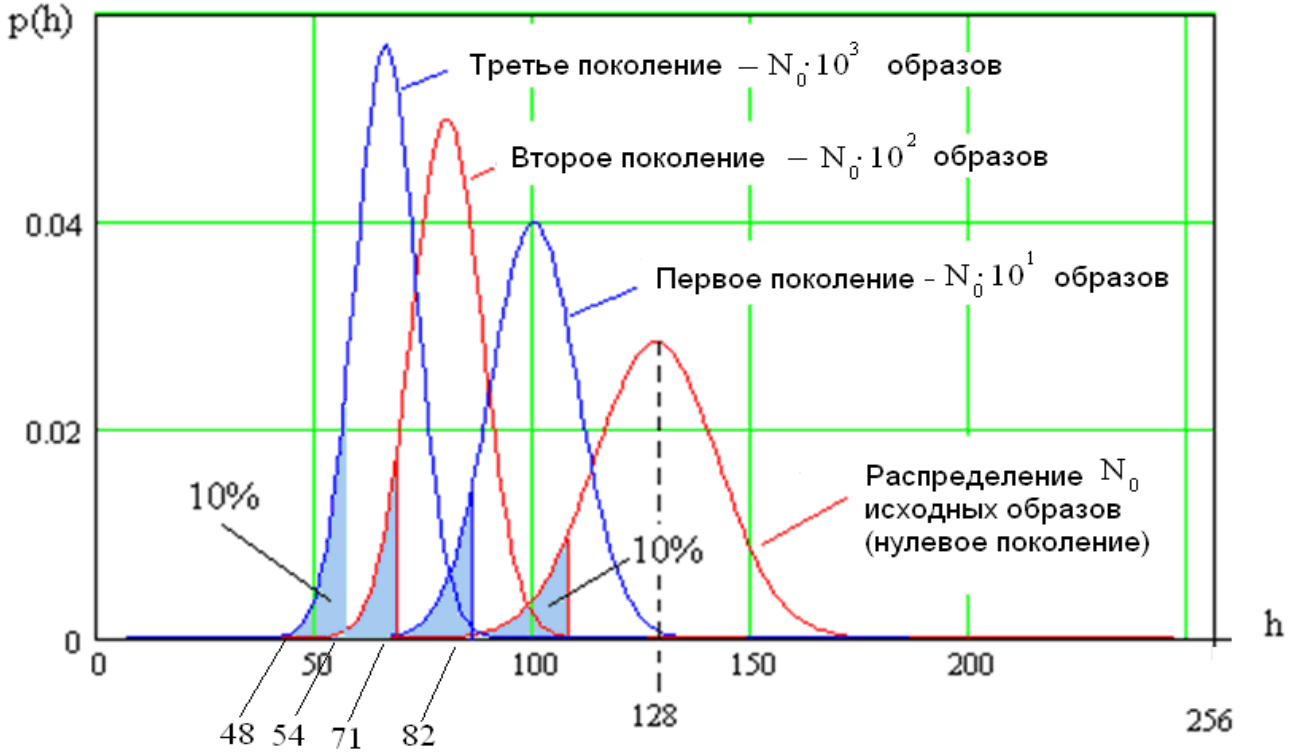


Рис. 20 Изменение распределений расстояний Хэмминга между кодом образа «Свой» и кодами «Чужие» при последовательной селекции направленных генетических модификаций нескольких поколений тестовых образов

Если преобразователь биометрия-код обучен правильно и тестирование ведется действительно случайными образами «Чужой», то математическое ожидание расстояний Хэмминга будет составлять 128 бит (половина длины выходного кода из 256 бит). Исходная плотность распределения значений расстояний Хэмминга (исходного нулевого поколения) тестовых

биометрических образов отображена в центре рисунка 20. Так как нам необходимо найти образы близкие к образу «Свой», из всех проверенных образов необходимо выбрать те, которые имеют минимальное значение расстояний Хэмминга. Рисунок 20 соответствует ситуации, когда из всей исходной выборки используют только 10% наиболее похожих образов.

Далее выборку из 10% наиболее похожих образов необходимо использовать как исходный материал для создания следующего (первого) поколения синтетических биометрических образов. Синтетические биометрические образы необходимо формировать из естественных биометрических образов по требованиям, изложенным в ГОСТ Р 52633.2-2010 [22]. Синтез новых биометрических образов осуществляют скрещиванием образов-родителей и получением от них образов-потомков. Скрещивание осуществляют последовательным линейным морфингом биометрических данных образов-родителей, параллельно осуществляют размывание данных образов-потомков мутациями (данными от генератора случайных чисел). Размножение синтетических биометрических образов ведут до момента, пока численность выделенных селекцией образов не восстановится до исходной численности нулевого поколения.

В конечном итоге, все примеры каждого следующего поколения образов «Чужой» оказываются намного ближе к образу «Свой» в сравнении с образами «Чужой» предыдущего поколения. То есть, плотность распределения значений расстояний Хэмминга для каждого нового поколения смещается в сторону нулевых расстояний, как это показано на рисунке 20. Процедуру селекции

наиболее похожих образов и их размножение, восстанавливающее численность популяции повторяют несколько раз. При этом удается восстановить от 75% до 95% биометрических данных образа «Свой», уже через несколько поколений генетической селекции.

Очевидно, что описанные выше процедуры генетического обращения матриц нейросетевых функционалов, являются трудоемкими (требуется формировать базу тестовых биометрических образов и ждать пока идет селекция, а также синтез нескольких промежуточных поколений биометрических образов). Существенно снизить трудозатраты удается, если вместо обычной меры Хэмминга (21) использовать взвешенную меру Хэмминга [24]. Во взвешенной мере появляется показатель стабильности того или иного разряда выходного кода «Чужой-i». Стабильные разряды кода оказывают более сильное влияние на меру, чем нестабильные. Абсолютно случайные разряды кода с нулевой стабильностью вообще не оказывают никакого влияния на значение взвешенного расстояния Хэмминга. В формуле используется показатель стабильности, введенный в ГОСТ Р 52633.5 [7].

Описанная выше процедура близка по своей идеологии тому, что мы называем естественным отбором по некоторой наиболее выгодной на данный момент комбинации биометрических параметров (биометрических признаков). Насколько этот тип итерационных процедур отражает реальные процессы, происходящие в природе, не известно. Тем не менее, на практике такой подход к поиску решений оказывается эффективным для

достаточно широкого круга прикладных задач [25, 26].

13. Связь избыточности кодов слов языка с уровнем его информативности

Известно, что все естественные языки обладают некоторой кодовой избыточностью. Брюс Шнайер [27], ссылаясь на Томаса Кавера [28] считает, что энтропия одной буквы английского языка составляет 1,3 бита для 16-ти символьных блоков текста. Если считать, что английский алфавит имеет 26 букв, то энтропия должна составить 4,7 бита на букву ($\log_2 26 \approx 4{,}7$ бит) для случайных, бессмысленных блоков текстов произвольной длины. То есть избыточность английского языка составляет 3,4 бита на букву или 260%.

Из-за того, что коды слов и фраз со смыслом на том или ином языке обладают избыточностью, появляются корреляционные связи между парами случайно выбранных разрядов этих кодов. Если бы коды не имели избыточности (были случайными), то коэффициенты корреляции между любыми парами разрядов оказались бы нулевыми $\left|r(x_i, x_j)\right| = 0.0$ для i≠j. Для избыточных кодов ситуация меняется $\left|r(x_i, x_j)\right| \rangle 0.0$ при i≠j. Для кодов с избыточностью следует вычислить математическое ожидание модуля корреляционных связей множества случайно выбранных пар разрядов выходного кода $r = E(\left|r(x_i, x_j)\right|)$. В этом случае высокоразмерная энтропия выходных кодов будет связана со средней входной энтропией каждого из разрядов следующим

соотношением:

$$H(x_1, x_2, ..., x_n) = (\beta(n,r) \cdot (n-1) + 1) \cdot E\{H(x_i)\} \qquad (22),$$

где $\beta(n,r)$ - это почти мультипликативный параметр, являющийся функцией двух переменных: числа разрядов – n и их корреляционной связанности – r. Эта двухмерная функция представлена номограммой на рисунке 21.

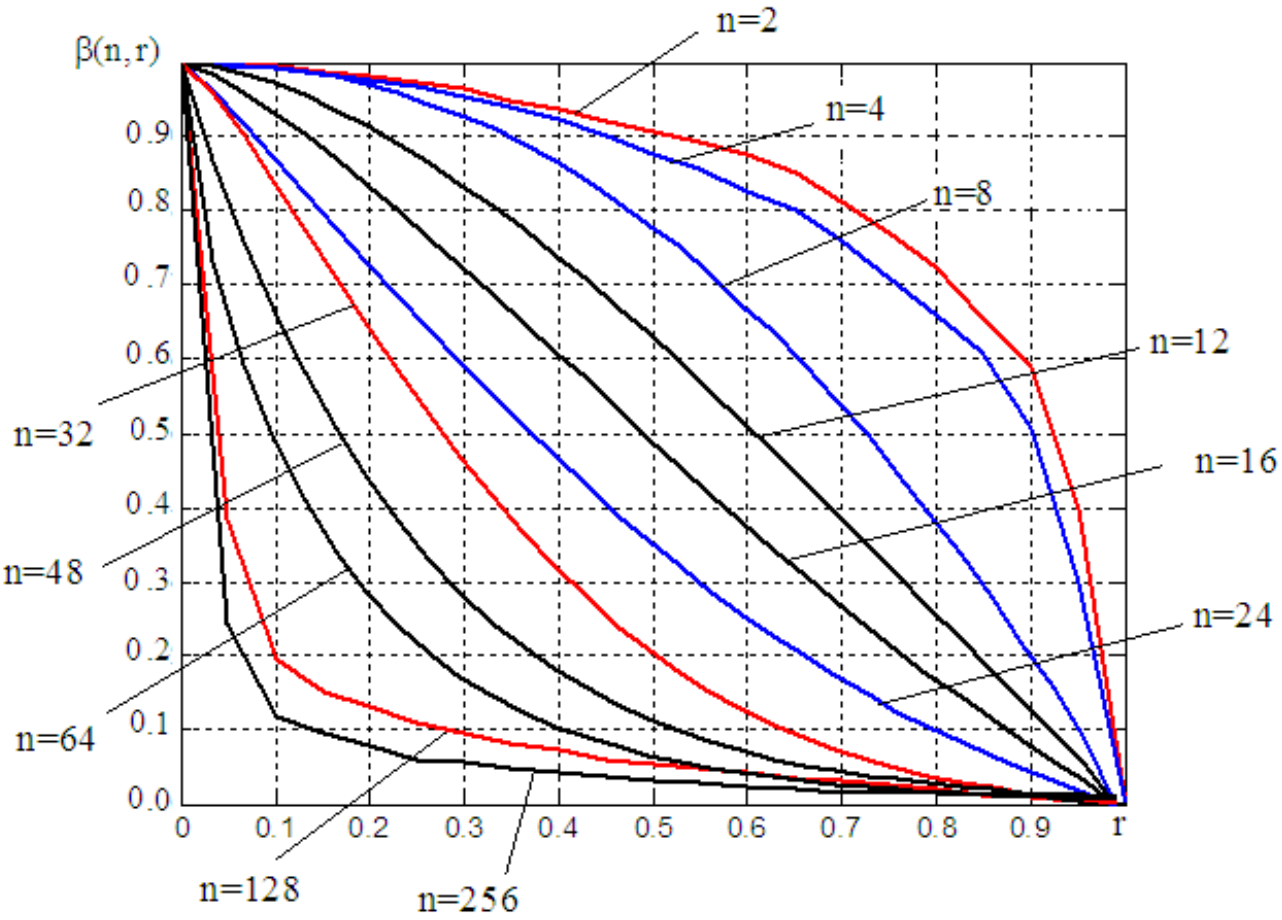


Рис. 21 Номограмма значений мультипликативной функции связи энтропии выходных кодов с коэффициентом равной коррелированности разрядов

Из рисунка 21 видно, что при небольших размерностях $n \leq 16$ многомерная энтропия ведет себя совершенно иначе, чем высоко-размерная энтропия для $n >> 16$. Для пограничной ситуации функция $\beta(16,r)$ почти мультипликативной связи оказывается

практически линейной.

Следствием качественных изменений функции $\beta(n,r)$ при переходе от низких размерностей к высоким размерностям является изменение отношения к оценке качества систем через контроль корреляционных связей между их параметрами. Для систем низкой размерности существенные корреляционные связи вполне допустимы, они практически не влияют на качество принимаемых нейронными сетями решений. Для систем высокой и сверхвысокой размерности все резко меняется, для них высокие корреляционные связи между контролируемыми параметрами уже недопустимы.

Через многомерные функции энтропии можно определить их многомерные корреляционные аналоги:

$$R(x_1, x_2,..., x_n) = (1 - \frac{H(x_1, x_2,..., x_n)}{n \cdot E\{H(x_i)\}}) \qquad (23).$$

При таком определении корреляционный функционал (23) всегда положителен и является дополнением классической функции многомерной энтропии. Максимум многомерной энтропии всегда соответствует минимуму многомерного корреляционного функционала. Связь корреляционного функционала (23) с классическими коэффициентами корреляции – r осуществляется через функцию $\beta(n,r)$.

Подчеркнем, что прямое вычисление высоко-размерной энтропии $H(x_1, x_2,..., x_n)$ и высоко-размерной корреляции $R(x_1, x_2,..., x_n)$ - это очень сложные в вычислительном отношении задачи, требующие огромных массивов исходных данных. Прямое

вычисление и $H(x_1, x_2,..., x_n)$, и $R(x_1, x_2,..., x_n)$ является технически невыполнимыми задачами. Вычисление же среднего значения модулей парных корреляций $r = E(|r(x_i, x_j)|)$ - это простая в вычислительном плане задача, для решения которой достаточно 1000 случайно выбранных длинных кодов с зависимыми разрядами. Рассчитывая параметр r и пользуясь номограммой рисунка 21, мы получаем чрезвычайно быстрый алгоритм оценки высоко-размерных значений энтропии и высоко-размерных коэффициентов корреляции. Если идти этим путем, то возникает выигрыш по времени вычислений, а так же по размерам тестовых выборок на десятки и сотни порядков. Все это выглядит фантастикой, но проверено на реальных биометрических высоко-размерных кодах и длинных блоках кодов текстов трех естественных языков [29] русский, английский, татарский.

Усредненная информативность кодов группы из n символов определяется следующим образом:

$$E\{I(x_1, x_2,..., x_n)\} = n \cdot E\{H(x_i)\} - H(x_1, x_2,..., x_n) \quad (24).$$

При необходимости от усредненной информативности, вычисленной по формуле (24), может быть осуществлен переход к информативности одной буквы алфавита, кодируемой несколькими разрядами кода. Так же может быть осуществлен переход к вычислению избыточности биометрических кодов (по аналогии с избыточности естественных языков). Расчеты показывают, что избыточность биометрических кодов сильно зависит от длины анализируемого блока кода и от качества самого биометрического образа. Современные нейросетевые преобразова-

тели биометрия-код, созданные в ОАО «Пензенский научно-исследовательский электротехнический институт» Концерна «Автоматика», дают избыточность от 600% до 1500%, что намного ниже информативности русского, английского или татарского языков. На данный момент пока не удается добиться качества нейросетевых преобразований искусственного подсознания биометрических автоматов, сравнимого с качеством нейросетевого подсознания естественного интеллекта человека.

14. Усилия России по противодействию «цифровой диктатуре» путем развития технологических предпосылок «цифровой демократии»

В настоящее время все развитые страны объявили о создании «электронного правительства» и своего стремления активно двигаться в направлении создания информационного общества или общества «знаний». При этом, инициаторами а так же идеологами всех этих процессов являются США и страны НАТО, а абсолютное большинство менее активных в создании новой идеологии стран занимают пассивную позицию молчаливой поддержки.

К сожалению, пассивная позиция большинства присоединяющихся стран делает страны-лидеры информатизации абсолютно защищенными от критики. Пользуясь своим доминирующим положением, IT-элита (IT олигархия) США и стран НАТО стремиться разрушить существующие нормы международного права и международной морали и навязать всем решения суда штата «Калифорния», как образец

для подражания. К сожалению, происходит открытое вмешательство США и стран НАТО во внутренние дела суверенных государств с помощью «гуманитарных бомбардировок» и отключения банкоматов в момент «цветных революций». Похоже, что подобные амбиции появились в истории человечества не впервые. Мы все уже многократно проходили через цифровые революции и смену одного общественного строя другим.

При изучении истории мы видим чередующиеся циклы нестабильности (хаоса) и стабильности, причем выход из хаоса, как правило, осуществляется через диктатуру как наиболее простую форму общественной организации. На рисунке 22 приведена иллюстрация основных исторических этапов развития человечества: матриархат, рабовладение, феодализм, капитализм, «информатизм» с наложением на них чередующихся циклов стабильности в форме демократии или диктатуры и хаоса.

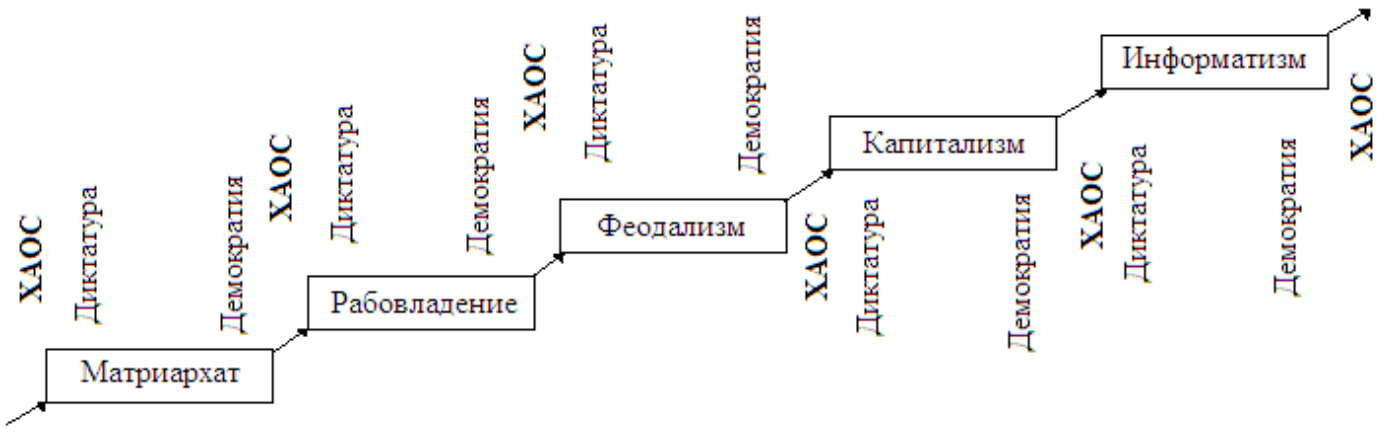


Рис. 22. Этапы развития общественно-экономических формаций, связанные со сменой общественных укладов, морали и права

Очевидно, что выделенные на рисунке 22 исторические эпохи являются достаточно стабильными образованиями

со сходными в рамках одной эпохи нормами: морали, права личности, межгосударственного права. То, что в эпоху рабовладения отвечало нормам морали и права, сегодня уже не является моральным и не соответствует нормам современного права как гражданского, так и международного. Во времена Рима иметь рабов было этично. Более того, было жесткое деление на граждан и рабов (не граждан). Сегодня иметь рабов (не граждан) является не этичным, однако существуют целые страны (Литва, Латвия, Эстония и территория Косово), где значительная честь населения является не гражданами (рабами в рамках Римского права). Высока вероятность того, что именно эти страны могут оказаться детонаторами нестабильности. То, что лишение гражданских прав существенной части населения является огромным дестабилизирующим фактором ни для кого не является секретом. Однако, НАТО демократия на это закрывает глаза, сейчас ей так удобно смотреть.

Следует отметить, что в рамках идеологии марксизма-ленинизма история рассматривалась как некоторое поступательное развитие производительных сил общества и отношения прав собственности на эти производительные силы. Возможен параллельный подход к исследованию исторических закономерностей, опирающийся на учет развития технологий извлечения знаний, их тиражирования, хранения, распространения во времени и пространстве. Нельзя точно указать что является первичным (знания или производительные силы), и что является вторичным? И знания и производительные силы являются отражением разных сторон одного и того же уровня развития

ЦИВИЛИЗАЦИИ. Без знаний нет развития производительных сил, без развития уровня наших возможностей (наших производительных сил) нет возможности эффективной добычи новых знаний.

Очевидно, что между стабильными эпохами развития цивилизации с похожими нормами морали и права возникают переходные периоды нестабильности, войн, хаоса. Обычно этот период наступает после эпохи демократии (рабовладельческой, феодальной, капиталистической). Сегодня мы находимся на этапе свертывания капиталистической демократии и скатывания в эпоху хаоса эпохи перехода в новое состояние - информационное общество (информатизм). Все современные политики говорят нам об угрозе «терроризма», однако, «терроризм» это синоним неустойчивости перехода в информационное общество. Если бы общество продолжало бы быть устойчивым, то никто не смог бы его раскачивать. Терроризм создается взаимными усилиями двух сторон: СМИ и террористов. Если бы СМИ в погоне за сенсациями не усиливали бы своим влиятием террористические акты, террор был бы полностью бесполезен с точки зрения его организаторов. Если нет массового психоза СМИ, то террористические акты оказываются абсолютно неэффективными и не могут повлиять на общественное сознание.

В нашем языке закрепились такие понятия как «электронная почта» и «электронное правительство». Параллельно с ними существует понятие «электронная цифровая подпись». С технологической точки зрения правильно было бы говорить «электронная цифровая почта» и «электронное цифровое

правительство», родной русский язык просто опускает такую подробность как «цифровая». Говоря «электронная почта» и «электронное правительство» мы упускаем из виду, что Интернет это только «цифровая» субстанция, там все в цифре. В ЭВМ и Интернете нет непрерывных данных, там все оцифровано. Цифровая почта говорить не менее верно, чем электронная почта, однако мы будем говорить именно электронная, так как это уже закрепилось в языке.

Рис. 23. Технологии распространения знаний в различных исторических эпохах, опирающиеся на формализацию знаний в той или иной цифровой форме

Если исходить из предпосылки, что язык и сформулированные на нем знания являются некоторой технологической основой обработки информации, то удается связать общепринятые исторические этапы общественного развития с определенными совершенствованиями технологий обработки информации. Связывание исторических эпох с технологическими нововведениями отображено на рисунке 23.

Из рисунка 23 видно, что «матриархат» следует рассматривать как период нехватки людей или период тиражирования общественных знаний (тиражирования людей как носителей общественных знаний). При этом главное - это то, кому общественное сознание доверяет функцию своего воспроизводства. Общество выбирает тех матерей, кому доверено иметь детей и чей общественный статус позволяет иметь много детей. Качество потомства наиболее просто прогнозируется по личным качествам их матери, прослеживать влияние отцов много сложнее. Судя по тому, что нас стало очень много, «матриархат» оказался очень эффективной политикой тиражирования наиболее достойных из нас и одновременного тиражирования общественных знаний, эффективными носителями которых являются наиболее достойные из нас.

Окончание «матриархата» наступает, когда людей становится больше, чем могут прокормить легко доступные природные ресурсы. Начинается конкуренция между людьми за природные ресурсы, самая жестокая форма конкуренции - это война. Уважение к матерям сменяется на уважение общественного сознания к ярким воинам (боярам). Успех того или иного военного

похода осуществляется по числу пленных (рабов). Наступает эпоха рабовладения, когда воевать оказывается важнее, чем работать.

При рабовладельческом строе происходит важнейшее технологическое нововведение – появляется письменность (рисунок 23). Фактически, происходит отрыв личных и общественных знаний от человека – их носителя. Человек, как носитель информации не может жить вечно и одновременно находиться в разных местах (знания, сформулированные на языке людей, являются информацией). Излагая, свои знания в рукописной форме, человек создает новые носители информации, которые могут существовать вечно и распространяться в пространстве (тиражироваться) без участия первоисточника знаний. Письменность – это последовательность оцифрованных звуков языка, зафиксированных на твердом носителе в виде последовательности букв некоторого алфавита (в западной традиции) или последовательность иероглифов, каждый из которых соответствует тому или иному понятию (восточная традиция).

Во времена феодализма совершенствуется технология тиражирования знаний в виде книг, параллельно происходит рост числа грамотных людей, способных писать и читать. В наиболее информационно развитых странах, например, таких как Русь наблюдается феномен всеобщей грамотности в сочетании с очень высоким уровнем демократии (новгородское вече полностью грамотного населения). В этот момент Россия оказывается информационным центром развития цивилизации, именно тогда зарождается идея третьего Рима.

При феодализме активно идет торговля, развиваются товарно-денежные отношения, ведется цифровая учетность гражданского и государственного имущества в денежном эквиваленте. Появляется класс буржуазии (капиталистов), который во время хаоса буржуазных революций захватывает власть и устанавливает свою диктатуру. Пользуясь неограниченной властью диктатуры, капиталисты активно разрушают мораль и право предшествующего феодального строя. При этом диктатура «дикого» капитализма создает невыносимые условия для абсолютного большинства других «угнетенных» классов (сословий) и закрепляет свою победу в виде новых норм морали и права «дикого» капитализма.

Для подавляющего большинства населения стран эпохи диктатуры «дикого» капитализма перегибы в деформации прежних норм морали очевидны. Практически вся интеллигенция того времени возмущена «дикостями» новой капиталистической морали. Дюма пишет «Трех мушкетеров», воспринимая их как образцы чести и достоинства по отношению ко множеству его современников, являющихся представителями диктатуры «дикого» капитализма. Диктатура «дикого» капитализма настолько сильно деформирует традиционные нормы морали и права, что делает общество неустойчивым. Мировые войны и почти мировая революция - это есть не что иное, как следствие «неустойчивости» капиталистического общества, порожденная неконтролируемой алчностью диктатуры «дикой» буржуазии.

В эпоху капитализма происходит ряд технологических изменений, связанных оперативностью доставки новой

общественно значимой информации потребителям (рисунок 23). В 19 веке появляются СМИ в виде газет, сокращается время транспорта информации по телеграфу. В середине 20 века получают активное распространение кино, телефон, радио, телевидение, создаются ЭВМ коллективного пользования. Все это способствует обузданию алчности «дикого» капитализма, который после его приручения превратился в капиталистическую демократию последней четверти 20 века.

В свою очередь капиталистическая демократия на наших с Вами глазах превращается в информационное общество. Толчком к этому служит тотальная персонализация ЭВМ и снятие проблем нехватки вычислительных ресурсов. Мы являемся свидетелями тотального использования персональных телефонов (персональных ЭВМ, предназначенных для оцифровывания и обработки голоса при его передаче по радиоканалу связи). Появление Интернета делает доступными огромные массивы оцифрованных знаний, видимо, в ближайшее время мы станем свидетелями появления персональных СМИ, ориентированных на личные интересы и пристрастия каждого из нас. В свою очередь огромные объемы цифровой информации, размещенные в сети Интернет, порождают необходимость в появлении специальных поисковых машин, осуществляющих сортировку и ранжирование знаний.

Главным признаком информационного общества является тотальная приватизация вновь полученных знаний и приватизация старых знаний, конвертированных в форму удобных программных продуктов для типовых ЭВМ. Если в эпоху классического

капитализма авторское право распространялось на литературные произведения и патенты, то в эпоху раннего информатизма IT олигархия стремиться распространить авторские права на любой цифровой контент. То, что недавно было бесплатным, сегодня кем-то приватизировано и за каждую цифровую копию нужно платить. Рушится старая мораль и право, а на их месте новая информационная олигархия пытается навязать всем нам новые правила игры, выгодные, прежде всего, наиболее развитым в информационном отношении странам. Наш мир стремительно двигается к «дикой» стадии информационного общества в форме цифровой диктатуры информационной олигархии.

Появление таких гигантов как Google, Microsoft, Intel являются яркими примерами того, что современные информационные олигархи уже сосредоточили в своих руках значительные информационные и материальные ресурсы. Информационная олигархия близка к тому, чтобы захватить реальную власть и сформировать свою диктатуру в ближайшем будущем, например, в такой стране как США. Армия нанятых ими юристов сумеет подвести законодательную базу и оправдать все требования информационных корпораций к обычным гражданам США и всего остального мира. Если принять позицию о превалировании национальных законов США над международными законами, то шансов у нас всех избежать «цифровой диктатуры» практически нет. Нам ее навяжут усилиями армии США и стран НАТО через «гуманитарные» бомбардировки и «демократические» войны. Однако, НАТО безнаказанно может бомбить только Ливию и навязать ей свое понимание демократии, бомбить безнаказанно

Россию НАТО пока не может.

Все было бы очень печально, если бы не было активной роли России в формировании баланса информационных интересов между новой цифровой олигархией и обычными гражданами. Крайне важным моментом для устойчивого развития нашей цивилизации является то, что в ближайшее время в России захватить власть новая цифровая олигархия не сможет. То есть, оставаясь по многим вопросами лидером информационного развития, Россия в ближайшее время сможет проводить независимую информационную политику и тем самым обеспечивать мировой информационный баланс интересов разных стран и разных групп населения этих стран.

Следует отметить, что выше была описана только общая тенденция наиболее вероятного развития событий. В реальности мир не такой однозначный. Параллельно с формированием в развитых странах очень сильной цифровой олигархии идут процессы противодействия ее всевластию. Параллельно с закрытыми кодами операционной системы Windows развивается операционная система Linux с открытыми кодами. Развитие Linux ветви операционных систем с открытыми кодами – это общественное противодействие сверх концентрации власти и информационных ресурсов в руках монополиста - Microsoft. Параллельно с усилиями мировой научно-технической общественности, предпринимают усилия и современные государства. Так в России принят 152 закон «О персональных данных», накладывающий весьма и весьма существенные ограничения на технологические вольности операторов,

предоставляющих населению «цифровые услуги».

К сожалению, производители информационных приложений и операторы «цифровых услуг», в погоне за прибылью мало заботятся о безопасности своих продуктов. Для них главное - как можно быстрее захватить свою долю информационного рынка. То на сколько безопасен их продукт или их «цифровые услуги» для подавляющего большинства информационных компаний является второстепенным. На данный момент дополнительные риски, обусловленные ошибками в программном обеспечении и сбоями технологий операторов цифровых услуг, законодательно никак не регламентируются. Именно по этой причине нужна более жесткая политика государств. Государства должны четко регламентировать требования к безопасности информационных услуг и программных приложений. Именно государство должно независимо оценивать дополнительные риски, возникающие при переводе тех или иных услуг в цифровую форму, и осуществлять сертификацию (лицензирование) программных продуктов и «цифровых услуг».

Одной из основных тенденций информационного общества является персонализация аппаратно-программных средств обработки цифровой информации. Персональные ЭЦВМ превратились в персональные цифровые телефоны, далее появятся персональные программы, ориентированные на удовлетворение и защиту информационных интересов только одной личности. Все мы разные, наши интересы различны и рано или поздно мы придем к ситуации, когда нам будут предлагать строго индивидуальные лекарства (синтезированные с учетом личного генотипа), а электронное правительство должно будет

подходить к каждому из нас ИНДИВИДУАЛЬНО. Мы перестанем быть безликой массой, соответственно, наши личные программы и автоматы (наше личное железо) должны уметь безошибочно нас узнавать.

Для решения этой задачи в США и России активно развиваются биометрические технологии. Пока только эти две страны имеют собственные (независимые) национальные политики по развитию средств биометрической идентификации и аутентификации личности. Отличительной особенностью национальной политики США является упор на развитие полицейской биометрии автоматизированного паспортно-визового контроля иностранных граждан, пересекающих границу страны. Для этой цели национальные институты стандартизации США (NIST и ANSI), разработали более 100 национальных биометрических стандартов. Часть из этих национальных стандартов США с 2002 года преобразуются в международные биометрические стандарты международной организацией по стандартизации ISO/IEC через подкомитет JTC1 SC37 (Биометрия).

Россия, так же как и все иные страны, заинтересована в развитии средств полицейского биометрического контроля иностранных граждан, пребывающих на ее территорию. В связи с этим, международные стандарты комитета ISO/IEC JTC1 SC37 гармонизируются российским национальным комитетом № 355 (Автоматическая идентификация) подкомитет №7 (Биометрическая идентификация). Сложившаяся ситуация по разработке биометрических стандартов отображена на рисунке 24.

Очевидно, что полицейская биометрия контроля иностранных

граждан не может решить фундаментальной проблемы повышения устойчивости информационного общества. Главным дестабилизирующим фактором низкой устойчивости информационного общества является тотальный обман всех, тиражируемый через Интернет и СМИ.

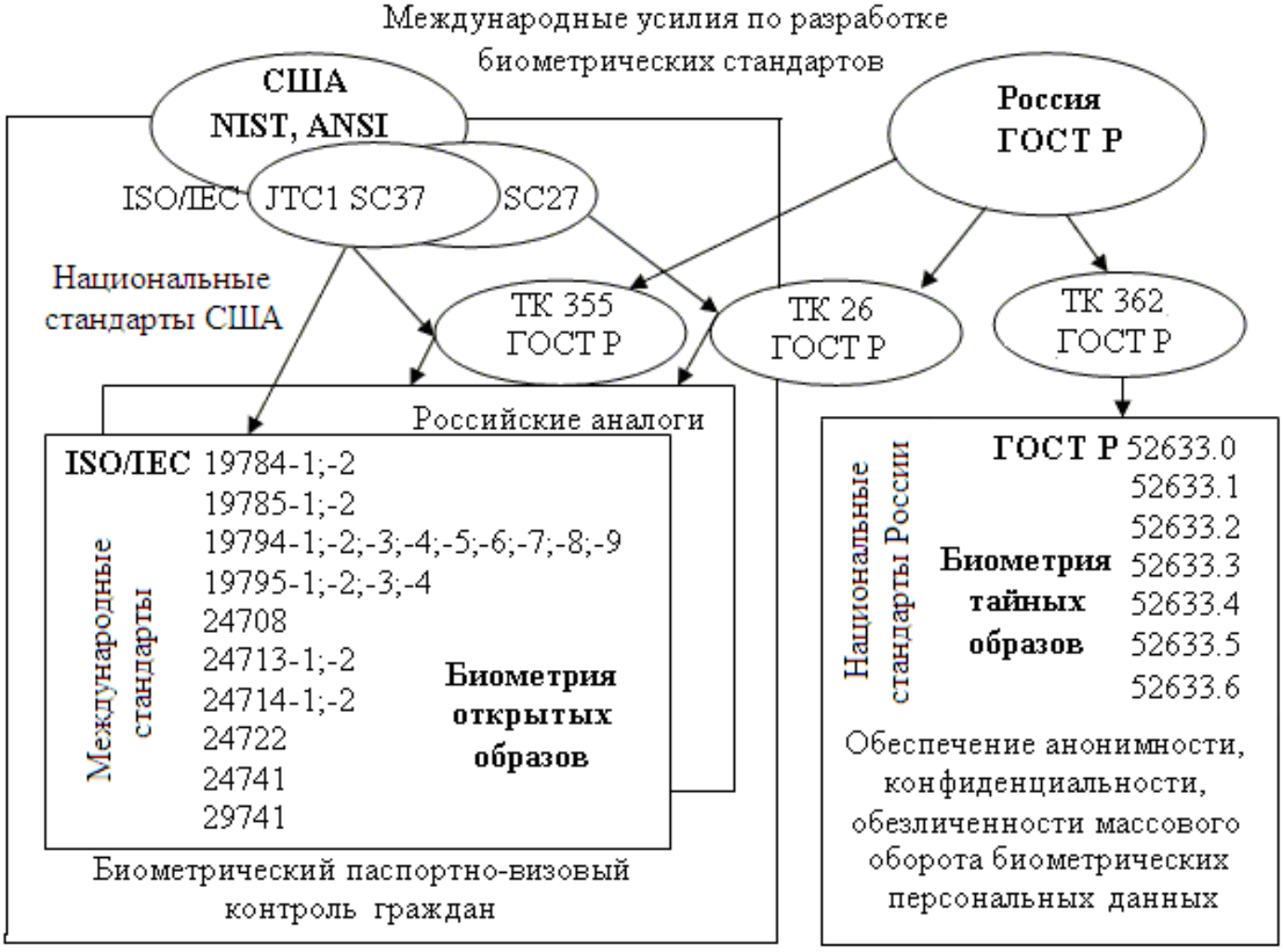


Рис. 24. Усилия США и России по созданию двух ветвей биометрических стандартов

Одной из причин массовой дезинформации является технологическая невозможность определить ее источник. Если бы в Интернете и средствах СМИ был повсеместно использован массовый электронный документооборот (все электронные

документы были бы охвачены электронной цифровой подписью), то найти и привлечь к ответственности человека-источника дезинформации, становится возможно. Однако это на данный момент является технологической утопией.

Проблема состоит в том, что обычные люди отторгают эту технологию. Информационные олигархи, например, операторы сотовой связи, активно используют технологию электронной цифровой подписи в своей практике. Их бизнес построен на инициировании SIM карт для сотовых телефонов их абонентов (в SIM карте находится важная информация, подписанная ЭЦП сотового оператора). Обычные люди стараются избегать технологии ЭЦП, так как не способны надежно хранить свой личный (секретный) ключ. Компрометация личного (секретного) ключа ЭЦП эквивалентна «цифровому рабству», куда попадает владелец скомпрометированного личного ключа. То есть для информационного олигарха формирование ЭЦП – это рутинная (безопасная) технологическая процедура, а для обычного человека – это очень опасная процедура. Это и есть суть «цифрового неравенства», крупные информационные компании могут пользоваться доверием общества, так как способны применять технологию ЭЦП. Обычные люди не могут оперативно получить доверие от общества, так как не способны надежно хранить свой личный ключ и оперативно использовать технологию ЭЦП.

В связи с этим современные государства должны обеспечить своих граждан средствами защиты их личного криптографического ключа. Только в этом случае возможен массовый электронный документооборот в открытых информационных пространствах с

участием в нем всех граждан. Полицейская (коллективная) биометрия для этих целей не подходит. Полицейская (коллективная) биометрия открытых биометрических образов людей подходит для паспортного контроля, для коллективного биометрического доступа в общественный подъезд дома, с открытым биометрическим образом может быть связан даже открытый ключ человека. Защитить свой личный (секретный) ключ можно только личной биометрией, которая способна сохранить в тайне биометрический образ человека. В биометрии работают те же основополагающие принципы, что и в криптографии: тайна намного сильнее технологии. Высоконадежная биометрическая защита личной информации может быть построена только на сохранении в тайне используемого человеком его биометрического образа: рукописного пароля, голосового пароля.

Именно технологии использования тайных биометрических образов активно развивает Россия, стремясь ликвидировать сложившееся «цифровое неравенство». В правой части рисунка 3 отображены номера пакета из семи национальных стандартов России, определяющих требования к средствам высоконадежной биометрической аутентификации личности человека, построенной на использовании тайны его биометрии. США и страны НАТО пока не создали ни одного национального стандарта, регламентирующего требования к биометрии тайных личных образов человека. Это связано, прежде всего, с изменением роли России, именно наша страна сегодня формирует технологический фундамент того, что позднее будет называться «цифровой демократией». Скорее всего, национальные стандарты России в

ближайшем будущем станут межгосударственными стандартами стран СНГ, а далее будут продвигаться как международные стандарты через ISO/IEC JTC1 SC27.

Сложилось вполне определенное международное разделение труда: США и страны НАТО активно создают полицейские биометрические стандарты открытых образов человека (лицо, рисунки отпечатков пальца, рисунок радужной оболочки глаза). Это происходит под активным давлением собственной информационной олигархии этих стран, активно стремящейся к захвату власти и своей диктатуре. Россия имеет гораздо более сбалансированную информационную политику формирования устойчивого информационного общества. Параллельно с полицейской биометрией общественного контроля за личностью, Россия активно формирует ветвь гражданской личной биометрии, использующей тайные биометрические образы человека. Это, видимо, связано с тем, что влияние на государство собственной информационной олигархии в России намного меньше, чем в США. Мы еще не ощутили всех прелестей «цифровой диктатуры», а Россия уже предпринимает меры по технологическому обходу этого капкана развития для всего человечества. Возможно, что усилия нашей страны позволят мировому сообществу развиваться, минуя этап «цифровой диктатуры» и сразу же закладывать технологические основы «цифровой демократии», создаваемого нами всеми информационного общества.

15. Требования к обучающим выборкам примеров биометрии коллективов людей и личной биометрии каждого

Одной из очень интересных особенностей организации биометрии человека является возможность объединения людей в рамках некоторых групп по биометрическим признакам, отражающим половые различия, расовые различия, генетическое сходство родственников, сходство речи носителей одного языка, сходство по профессиональным навыкам и так далее. Наиболее простым является деление людей по половым признакам: мужчины и женщины имеют существенно отличающиеся тела, разные черты лица и разный склад ума. Очевидным является то, что у женщин выше тональность голоса и темп речи, они ниже ростом. Мы легко отличаем акцент характерный для носителей другого языка. По речи человека можно локализовать страну и географический район его проживания, социальную группу к которой он относится, возраст человека, черты его характера.

Для теории подсознательного искусственного интеллекта крайне важно ответить на вопрос о том, должно ли подсознание дообучаться под особенности речи незнакомого нам человека, которого мы слышим в первый раз и хотим понять. Да, мы способны эффективно распознавать голоса знакомых нам людей. Помогает ли это нам понимать их речь? Можно ли построить распознаватель речи некоего среднестатистического голоса говорящего на русском? Выгодно ли деформировать среднестатистические настройки нейронной сети под особенности речи конкретного человека или проще обучать искусственное

подсознание с нуля особенностям голоса незнакомца?

Из практики известно, что эксперт-человек не способен узнавать одну букву (один звук) вырезанный из слитной речи, однако вырезанные из слитной речи предлоги и отдельные слова человек уже начинает понимать. При этом осмысленный текст из нескольких слов произнесенных одним диктором правильно понимается слушателем намного надежнее, чем изолированные слова. Если же давать эксперту для прослушивания последовательность слов, произнесенных разными людьми, способность эксперта понимать предъявленную последовательность звуков резко снижается.

Скорее всего, каждый из нас имеет специальные достаточно инерционные механизмы настройки на биометрические параметры речи собеседника. Видимо, наш слух в первые моменты восприятия чужой речи настраивается воспринимать частоту основного тона речи незнакомого диктора, темп речи выбранный говорящим и динамический диапазон частот его голосового аппарата. Искусственный интеллект современных вокодеров так же настраивается на частоту основного тона диктора, а вот настройку на темп речи вокодеры не производят, так как занимаются исключительно только кадровой обработкой звука. До совместной обработки нескольких кадров одного и того же звука или пары звуков искусственный интеллект существующих вокодеров пока не дорос. Современные вокодеры так же не учитывают динамический диапазон речи, воспроизводимой голосовым аппаратом того или иного диктора.

Все выше изложенное позволяет утверждать, что слушающий

диктора человек и, соответственно, искусственный интеллект следующего поколения вокодеров должен решать две задачи [30]: первая задача состоит в понимании содержания речи с учетом особенностей произношения звуков в рамках норм того или иного языка, вторая задача состоит в узнавании особенностей голоса знакомого диктора. Видимо, первая задача учета правил коллективной биометрии людей, говорящих на одном языке, выполняется сознанием и относится к задачам низкой размерности. Вторая задача, скорее всего, является высоко-размерной и должна решаться подсознанием естественного или искусственного интеллекта.

На сегодняшний момент надежную оценку размеров обучающей выборки мы можем дать только для подсознательной (нейросетевой) части биометрических вокодеров. Если биометрические вокодеры будут крайне примитивными и будут состоять из обычного вокодера и биометрического автомата аутентификации личности по фиксированной голосовой фразе, то для его обучения потребуется предъявить порядка 20 примеров заданной голосовой фразы. Практика показала, что аутентификация оказывается достаточно надежной, если длина фиксированной голосовой фразы составляет три слова длинной от 4 до 9 букв. При средней длине слова 7 букв получается, что для успешного обучения искусственного подсознания био-вокодера требуется произнесения диктором «Свой» текста примерно из 420 букв (звуков) или примерно 10 строк текста.

Если идентифицировать диктора необходимо на произвольном тексте, то придется использовать пары наиболее

часто встречающихся в языке звуков. По данным, приведенным в работе [31], вероятность наиболее часто встречающихся пар букв русскоязычного текса составляет величину близкую к 0,01. То есть, для получения от 10 до 20 примеров часто встречающихся пар звуков (букв), потребуется использовать произвольный обучающий текст длинной от 1000 до 2000 букв (звуков). При темпе речи 10 звуко-букв в секунду необходимо будет иметь образец речи диктора длинной от 100 до 200 секунд (от 1,7 до 3,3 - минут).

Если исходить из предположения, что сознательная часть вокодера должна решать задачу примерно в 100 раз меньшей размерности, то для ее настройки на особенности голоса неизвестного диктора должны потребоваться гораздо меньшие объемы исходной информации. Предположительно, для настройки на частоту основного тона диктора, его темп речи и его личный динамический диапазон частот огласованных звуков потребуется порядка 32 звуко-букв. Косвенно правоту этого утверждения подтверждает национальный стандарт ГОСТ Р 51061-97 [32], именно столько звуко-букв имеют наиболее короткие тестовые фразы, рекомендуемые этим стандартом.

16. Экономичное вычисление высоко-размерной энтропии естественных языков на очень маленьких вычислительных машинах

Следует отметить, что наша с Вами письменность – это кодировка речи на нашем естественном языке буквами. Каждая буква далее может быть оцифрована, например, в кодировке ASCII. Очевидно, что по кодам русскоязычных текстов мы

можем вычислить энтропию русского языка по формулам (1), (2), (3). При этом нам потребуется текст примерно из 1000 знаков для вычисления энтропии одного знака $H(x_1)$. Для вычисления энтропии появления пар букв в русском языке $H(x_1,x_2)$ потребуется примерно 32 000 знаков (16 страниц текста). Для вычисления энтропии появления троек букв в русском языке $H(x_1,x_2,x_3)$ потребуется примерно 1 000 000 знаков (500 страниц текста). По индукции можно показать, что для вычисления энтропии появления сочетаний из 32 букв в русском языке $H(x_1,x_2,\ldots,x_{32})$ потребуется примерно 10^{47} знаков. Оцифрованных текстов на русском языке столь огромной длины 10^{47} знаков может и не оказаться в ближайшей библиотеке. Нет так же в городе Пенза вычислительных машин для осуществления расчетов энтропии по Шеннону за приемлемый интервал времени на столь значительных объемах данных.

В связи с этим энтропию по Шеннону не считают более чем для групп из 8 знаков (кодов длиннее 64 бит) естественного языка. Эта ситуация никого особо не тревожила в прошлом веке и в начале этого века. Однако, в 2004 году в России в рамках НИР «Нейросеть» появились нейросетевые преобразователи рукописных паролей в личный код пользователя длинной 256 бит. Если воздействовать на нейросетевой преобразователь биометрия-код случайными образами «Чужой», то на его выходе появятся случайные коды. Эти коды имеют существенно коррелированные разряды (не являются белым шумом). В связи с этим возникла задача тестирования стойкости преобразователя биометрия-код к атакам подбора, которая эквивалентна

вычислению энтропии выходных случайных кодов. Если идти обычным путем классического вычисления энтропии по Шеннону, то задача оценки стойкости преобразователей биометрия-код к атакам подбора оказывается очень сложной. Для упрощения задачи было предложено воспользоваться распределением расстояний Хэмминга между кодом «Свой» и случайными кодами «Чужой» [9, 10]. Аналогично можно поступать и с кодами текстов на русском языке. Пример вычисления расстояния Хэмминга между кодами букв «а» и «х» приведен ниже:

1 1 1 0 0 0 0 0 ⟶ код "а" (224)
⊕⊕⊕⊕⊕⊕⊕⊕
1 1 1 1 0 1 0 1 ⟶ код "х" (245)
———————
0 0 0 1 0 1 0 1 ⟶ 3 бита - расстояние Хэмминга

Совершенно так же может быть вычислено расстояние Хэмминга между кодами любых букв в тексте. Более того, мы можем взять код буквы «а» и вычислить распределение его расстояния Хэмминга до всех букв некоторого текста. Пример такого распределения приведен на рисунке 25.

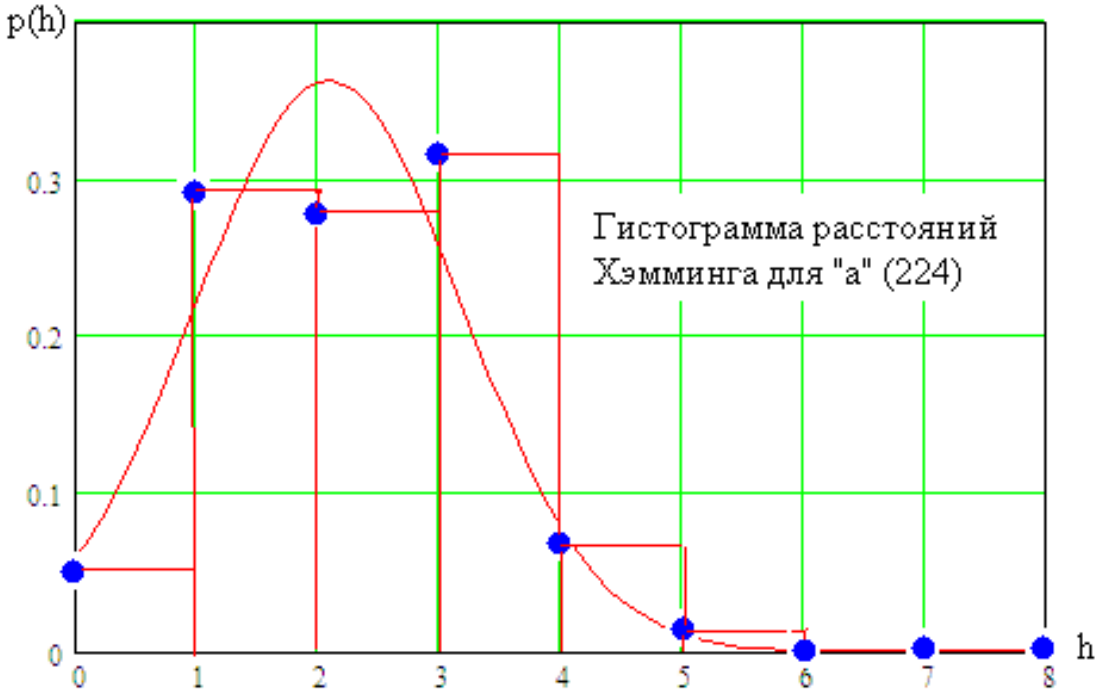


Рис. 25. Пример гистограммы распределения расстояний кодов Хэмминга между кодом буквы «а» (224) и кодами букв текста на русском языке в кодировке ASCII

Рисунок 25 иллюстрирует то, что вероятность появления кода «а» в анализируемом тексте может быть вычислена как отношение площади крайнего левого столбца гистограммы к общей сумме площадей всех столбцов:

$$P = \frac{p(h_0)}{\sum_{i}^{n} p(h_i)} \quad (25),$$

где n-длина сравниваемых кодов, $p(h_i)$ – высота столбца гистограммы.

Так же следует отметить, что гистограмма рисунка 25 существенно отличается от нормального закона распределения значений. Однако, если мы начнем вычислять распределение расстояний Хэмминга для пары букв, то оно окажется намного

ближе к нормальному закону, как это показано на рисунке 26. По мере роста числа букв или по мере роста длины сравниваемых кодов происходит быстрая нормализация распределений расстояний Хэмминга. Как видно из рисунка 26 уже для двух букв распределение кодов Хэмминга оказывается почти нормальным, для групп из трех, четырех и более букв распределение расстояний Хэмминга становится еще ближе к нормальному. Это означает, что вероятность появления той или иной последовательности букв можно вычислить по следующей формуле:

$$P = \frac{1}{\sigma(h) \cdot \sqrt{2\pi}} \cdot \int_0^1 \exp\left(\frac{-(E(h) - u)^2}{2 \cdot (\sigma(h))^2}\right) \cdot du \qquad (26),$$

где E(h) – математическое ожидание расстояний Хэмминга исследуемой группы кодов букв по отношению к последовательности кодов текста; $\sigma(h)$ – стандартное отклонение расстояний Хэмминга.

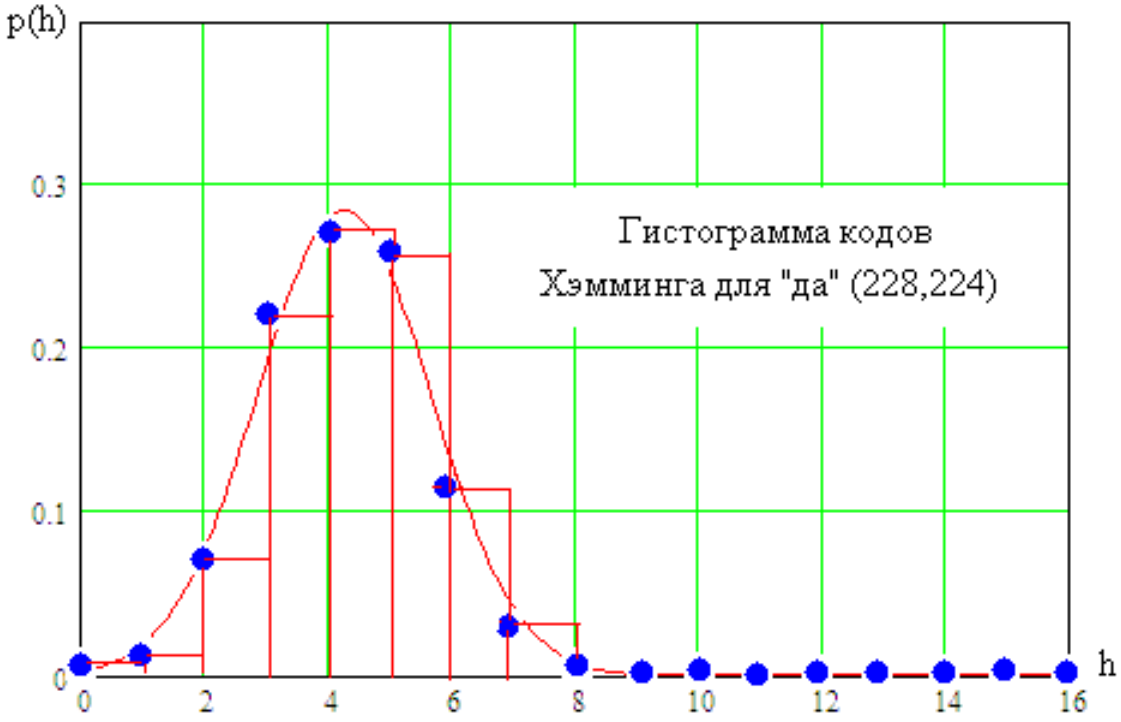


Рис. 26 Гистограмма распределения расстояний Хэмминга между кодом пары буквы «да» (228 224) и кодами пар букв текста на русском языке в кодировке ASCII

Следует подчеркнуть, что математические выражения (25) и (26) оценивают одну и ту же вероятность, но имеют совершенно разный технический смысл. Если мы используем выражение (25), то мы обязательно должны наблюдать в тексте появление той или иной последовательности букв. Если мы будем пользоваться выражением (26), то нам нет необходимости наблюдать последовательность букв в тексте. Из-за этого удается оценивать вероятности появления последовательностей из 32 букв на текстах всего из 1 000 букв. Выборки из 1 000 знаков вполне достаточно, что бы точно оценить математическое ожидание и стандартное отклонение расстояний Хэмминга, используемых в формуле (26). Используя при расчетах энтропии зависимых кодов распределение расстояний Хэмминга, фактически удается получить очень

значительное ускорение вычислений. Ускоритель вычислений Хэмминга дает выигрыш по вычислительным затратам в сравнении с процедурами Шеннона тем больше, чем длиннее исследуемые коды (чем более длинную последовательность букв мы исследуем). Возникает так называемый эффект «благодати» высоких и сверхвысоких размерностей. Вместо понятного всем «проклятия» размерности появляется инверсия этого эффекта в форме «благодати» высоких и сверхвысоких размерностей.

Следует отметить, что достигнуть ускорения вычислений на несколько десятков порядков удается не только путем предсказания вероятности появления редких событий по формуле (26). Можно идти другим путем, через вычисление коэффициентов парной корреляции разрядов исследуемых длинных кодов. Для достаточно надежной оценки коэффициентов парной корреляции достаточно всего 1 000 примеров. Если усреднить модули вычисленных коэффициентов корреляции и воспользоваться номограммой рисунка 21 (стр. 61) мы можем вычислить энтропию на еще меньшей выборке данных, применив преобразование (23) стр. 62. Естественно, что этот дополнительный выигрыш в ускорении вычислений может быть достигнут только при условии высокого доверия к данным номограммы рисунка 21. В этом отношении использование формулы (26) и классических процедур Шеннона более предпочтительно, так как не нуждается в доверии к номограмме рисунка 21.

Следует обратить особое внимание на то, что вычисление высокоразмерной энтропии естественных языков может быть осуществлено на маленьких вычислительных машинах.

Необходимость в больших вычислительных машинах отпадает. Та же самая ситуация возникает и при вычислении высоко-размерной энтропии других систем, например, при вычислении энтропии реальных газов без угрозы возникновения в расчетах парадокса Гиббса [33].

Сегодня обход парадокса Гиббса выполняется двумя путями. Первый путь предложен самим Гиббсом [33]. Он прост, но никак не обоснован со стороны здравого смысла. Второй путь состоит в моделировании на вычислительной машине взаимодействия молекул газа между собой и стенками сосуда. Второй путь крайне трудоемкий, нужны большие вычислительные машины и физически достоверные модели взаимодействия миллиардов молекул того или иного реального газа. Воспроизведение физических моделей миллиардов молекул с учетом ограничений в виде стенок сосуда требует очень больших вычислительных ресурсов. При таком подходе вычислительных ресурсов всегда будет мало, вычислительные машины всегда будут перегружены, а результаты всегда будут скромны. Это и есть «проклятие» размерности в явной форме.

Для того, чтобы обойти «проклятие» учета взаимодействия миллиардов физических моделей молекул реального газа, необходимо выполнить примерно такой же маневр, как при вычислении энтропии естественных языков. Нужно поставить специальный эксперимент и измерить пространственные корреляции, возникающие при взаимодействии несимметричных молекул реального газа. Если не удается измерить корреляции прямым экспериментом, то следует их рассчитать на физически

достоверных моделях. Далее следует увеличивать размерность задачи, учитывая заданные показатели корреляции между состояниями молекул до взаимного соударения и после взаимного соударения. Если при этом используется номограмма взаимодействия подобная номограмме рисунка 21 (стр. 61), то все вычисления можно проводить на маленьких вычислительных машинах. Привлекать большие вычислительные машины, обслуживаемые большим штатом сотрудников, а также долго ждать и тратить много электроэнергии на их работу нет смысла. Вся работа может быть выполнена на обычной настольной вычислительной машине за приемлемый интервал времени.

17. Модификация схемы испытаний Бернулли: приближения биномиального закона распределения значений зависимых опытов

Подчеркнем, что для «белого шума» вообще не возникает проблем с оценкой вероятности появления тех или иных событий. Триста лет назад Бернулли придумал схему испытаний с бросанием одной монеты и вывел биномиальный закон расчета вероятностей появления тех или иных событий по угадыванию заданного числа состояний кода. К сожалению, в биометрии и других задачах полной независимости (идеального «белого» шума) не бывает. Всегда возникают существенные корреляционные связи и они очень сильно влияют на собственную энтропию исследуемой системы. Проверить это достаточно просто путем численного эксперимента [9], задавая равные значения коэффициентов корреляции между всеми моделируемыми

биометрическими параметрами. Результаты численного эксперимента отображены на рисунках 27 и 28. Формулы, связывающие между собой значения равных коэффициентов корреляции между моделируемыми параметрами и соответствующими статистическими показателями плотности распределения расстояний Хэмминга, даны в работе [18].

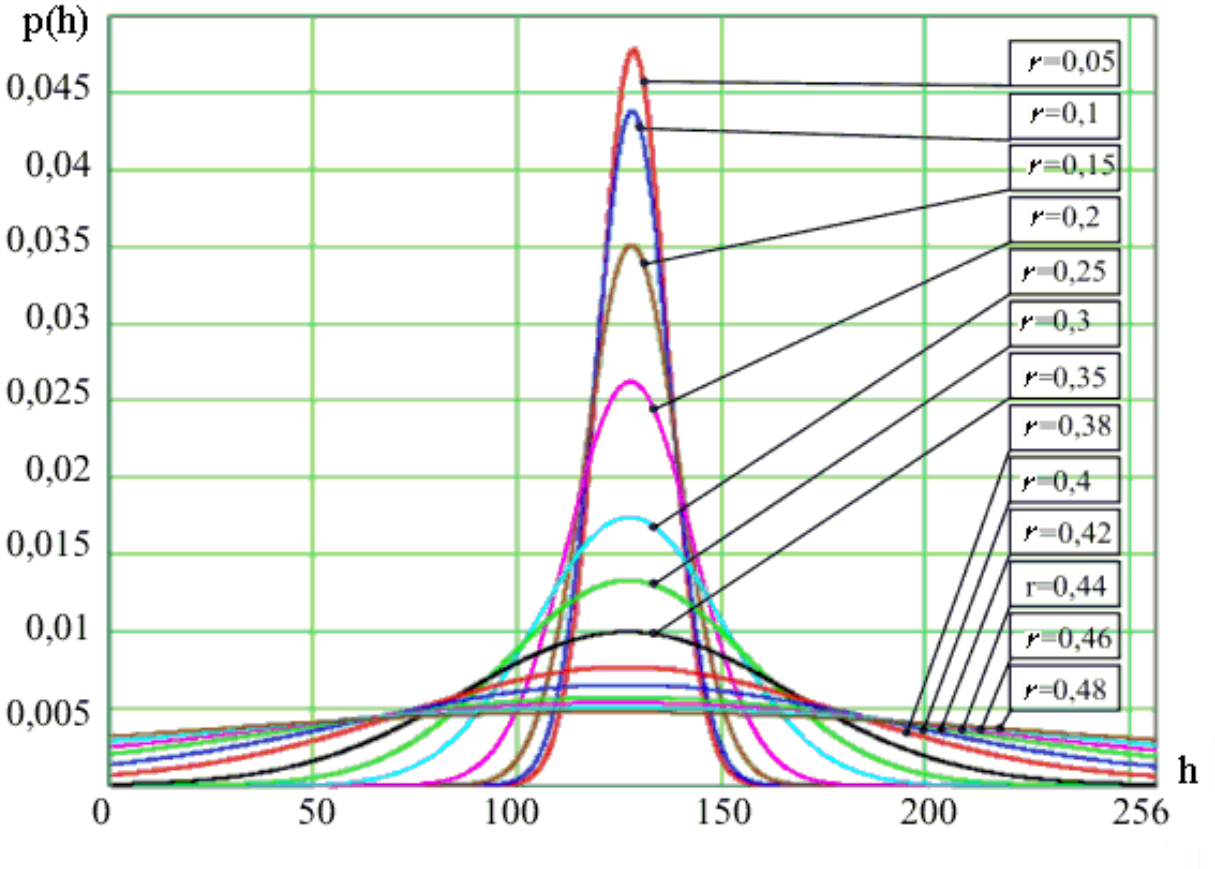


Рис. 27 Эволюция плотности распределения значений меры Хэмминга при монотонном росте модуля корреляционных связей между выходными разрядами кодов преобразователя

Из рисунка 28 видно, что при малых значениях модуля коэффициентов корреляции между выходными разрядами кодов преобразователя в пределах от r=0.0 до r=0.37 плотность распределения значений меры Хэмминга хорошо повторяет форму нормального закона распределения значений. Далее, в интервале

от r=0.37 до r=0.5, нормальный закон очень быстро превращается в равномерное распределение. При r=0.5 плотность распределения значений точно совпадает с равномерным законом (рисунок 28). Далее, при модуле коэффициента корреляции, изменяющемся в интервале от 0.5 до 0.63, равномерный закон распределения превращается в распределение арксинуса.

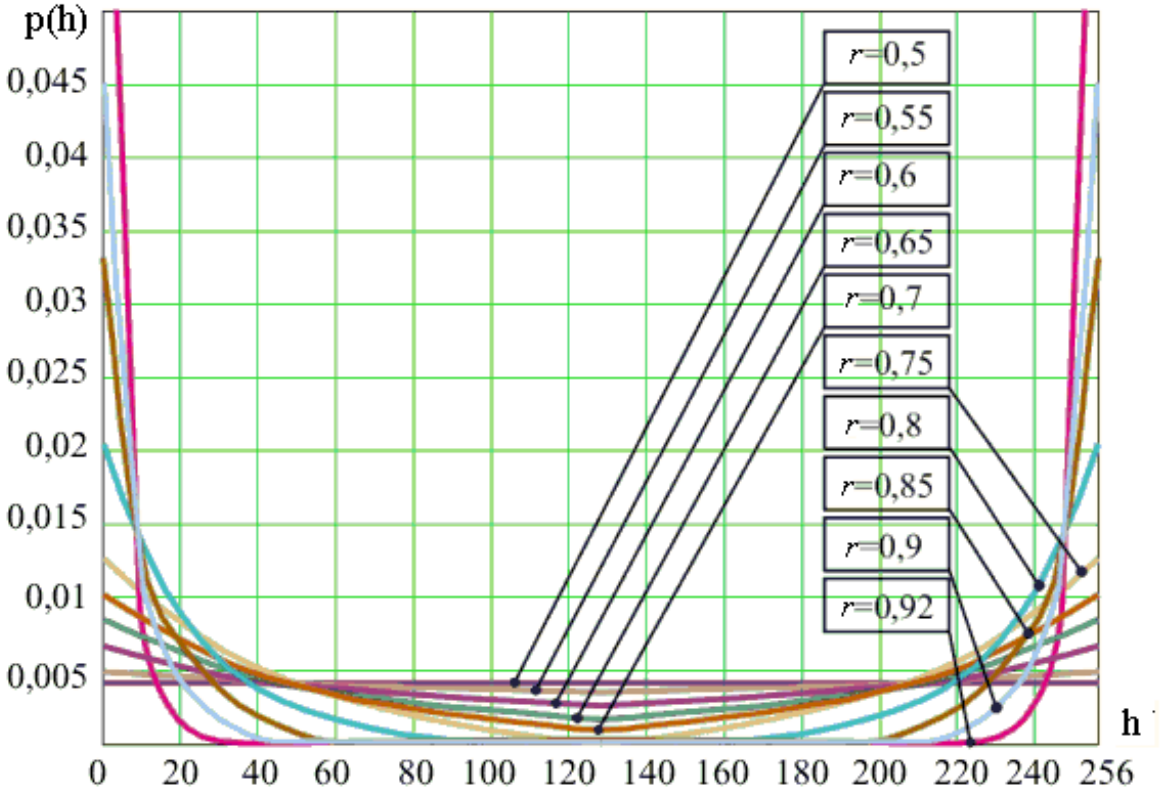


Рис. 28 Эволюция плотности распределения значений меры Хэмминга при монотонном росте модуля корреляционных связей в пределах от r=0.5 до r=0.92

Получается, что при монотонном росте модулей корреляционной связи в интервале от r=0.0 до r=0.63 форма закона распределения значений меры Хэмминга эволюционирует проходя три разных закона распределения: нормальный закон, равномерный закон и закон арксинуса. Формы всех трех этих законов приведены на рисунке 29.

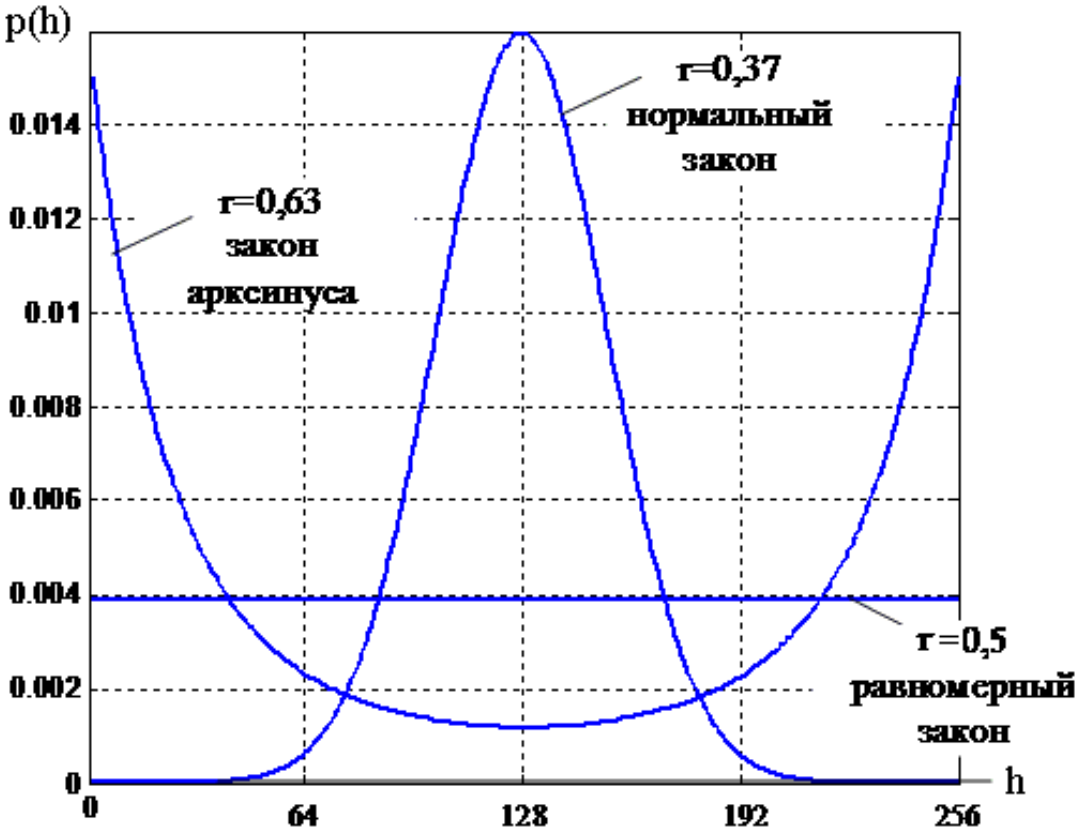


Рис. 29 Формы трех классических законов, являющихся этапами эволюции биномиального закона распределения значений зависимых данных.

Для того, чтобы получить приближение биномиального закона распределения значений расстояний Хэмминга между зависимыми кодами с корреляцией в интервале от |r|=0.0 до |r|=0.37, вполне достаточно нормального закона распределения значений.

В том случае, когда исследуемые коды оказываются более зависимыми (их усредненный модуль корреляций между разрядами находится в интервале от |r|=0.37 до |r|=0.5), необходимо использовать приближение в форме линейной комбинации нормального закона распределения и равномерного закона распределения значений расстояний Хэмминга.

В том случае, когда исследуемые коды оказываются еще более

зависимыми (их усредненный модуль корреляций между разрядами находится в интервале от |r|=0.5 до |r|=0.63), необходимо использовать приближение в форме линейной комбинации равномерного распределения расстояний Хэмминга и распределения по арксинусу. При корреляциях более |r|=0.63 хорошее приближение дает распределение по арксинусу, возведенное в некоторую степень. Показатель возведения в степень является подбираемым параметром аппроксимации.

Описанная выше аппроксимация приближенно описывает одну из модификаций традиционной схемы испытаний Бернулли. По этой модификации бросают не одну монету, а сразу горсть из 256 монет. Естественно, что конечное состояние каждой из монет уже нельзя считать независимым от состояний других монет.

Возможно использование еще более сложной модификации схемы испытаний Бернулли, по которой каждая из монет имеет свою асимметрию. В этом случае математическое ожидание расстояний Хэмминга всегда оказывается отличным от 128 бит. Учет этого факта приводит к незначительному усложнению аппроксимаций.

18. Оценивание устойчивости рынка через учет множества одномерных показателей Херста и взаимной коррелированности данных

Очень многие задачи реальной жизни нам кажутся случайными только из-за того, что мы не имеем возможности учитывать множество влияющих на них переменных. По мере того, как мы увеличиваем размерность задачи, неопределенность снижа-

ется и мы имеем все более и более детерминированное решение. В частности, это все остается справедливым и для задачи оценки (прогнозирования) показателей устойчивости рынка.

В настоящее время сложность оценки текущего состояния рынка и прогноза его будущего состояния объясняется фрактальностью задачи [34, 35]. Фрактальность или дробная размерность оказывает ощутимый эффект даже применительно к одному из показателей рынка (например, по отношению к колебаниям индекса S&P500 или любого иного индекса). В биометрии переход от учета одного параметра к учету множества параметров усиливает фрактальные эффекты [9]. Можно предположить, что для рынка также характерно усиление эффектов фрактальности по мере роста размерности задачи.

Приведенное выше сопоставление двух разных задач анализа рынка и биометрии человека является далеко не случайным. Видимо рынок является не чем иным как коллективной биометрией взаимодействия множества людей (покупателей и продавцов). Наиболее ярко эта идея отражена в гипотезе Ваге [36] когерентных рынков, которая построена на основе теории социальной имитации Калана и Шапиро [37]. В свою очередь состояния когерентного рынка очень похожи на состояния нейросетевого преобразователя биометрия-код, который в состоянии «Свой» имеет нулевую размерность (ноль степеней свободы), и нулевую неопределенность (нулевую энтропию). Однако, по мере отхода от состояния «Свой» в сторону любого состояния «Чужой», энтропия системы резко увеличивается и преобразователь биометрия-код начинает хорошо описываться

нормальным законом распределения значений. В переводе с языка биометрии на язык рынка «нулевое» состояние это обвал рынка и паника, все хотят одного и того же продать (купить), но никто не покупает (не может продать), рынок полностью когерентен. Состояние высокого значения энтропии наоборот свидетельствует о высоком уровне баланса противоположных желаний покупать и продавать, при этом рынок имеет очень высокий уровень собственной энтропии и высокий уровень размерности (рынок имеет минимальную для себя когерентность).

Биометрия как наука уже имеет высоко-размерную модель связи энтропии одного выхода с энтропией множества зависимых выходов [38, 39] (рис. 21 стр. 61). Соответственно, эта модель может быть применена к рынку. В итоге, мы сможем контролировать текущую энтропию рынка по десяткам и даже сотням доступных для контроля параметров.

Для биометрии весьма перспективным является заимствование у экономики статистической теории R/S анализа данных и вычисления по ним показателя Херста [34, 35]. Попытки применения R/S статистического анализа были предприняты с целью выявления скрытых колебаний психофизического состояния человека путем анализа стабильности его рукописного почерка. Использовались биометрические данные в виде коэффициентов ряда Фурье колебаний пера по двум координата x(t), y(t), получаемых при многократном воспроизведении человеком одного и того же рукописного слова. Из-за естественной нестабильности динамики почерка по каждому контролируемому биометрическому параметру получается ряд отсчетов (один отсчет

соответствует одной из попыток воспроизвести рукописно заданное слово-пароль).

При анализе данных осуществлялось классическое накапливание центрированных параметров:

$$V_i = \sum_{i=0}^{N} (v_i - E(v)) \qquad (27),$$

где v_i - значения контролируемого параметра; $E(v)$ - математическое ожидание контролируемого параметра.

Далее вычислялся нормированный размах накопленных значений:

$$R/S = \frac{\max(V_i) - \min(V_i)}{\sigma(v)} \qquad (28),$$

где $\sigma(v)$ - среднеквадратическое отклонение контролируемого параметра.

Показатель Херста вычислялся следующим образом:

$$H = \frac{\log(R/S)}{\log(N) - \log(a)} \qquad (29),$$

где N – окно наблюдения данных; а- константа, вычисляемая через использование разных значений окна наблюдения.

Из теории известно, что показатель Херста может изменяться в интервале от 0.0 до 1.0. При значении H=0.5 анализируемые данные являются независимым белым шумом с нулевой автокорреляционной функцией. Кроме того, зная показатель Херста, мы можем вычислить фрактальную размерность исследуемого процесса:

$$D = 2 - H \qquad (30).$$

В случае H=0.5 фрактальная размерность составляет D=1.5, при H=1 фрактальная размерность минимальна D=1, для H=0 фрактальная размерность максимальна. Формально, фрактальную размерность можно рассматривать как некоторый аналог энтропии исследуемого параметра рынка. Тогда состояние D=1 будет соответствовать полностью когерентному рынку или его обвалу. С другой стороны, любое увеличение фрактальной размерности контролируемого параметра должно свидетельствовать о росте его устойчивости (падении уровня когерентности). То есть, контролируя текущее состояние фрактальной размерности рынка по одному или нескольким параметрам мы можем судить о изменении ситуации и можем наблюдать куда движется рынок: в сторону когерентности поведения его участников или в сторону роста его внутренней энтропии (независимости поведения участников рынка).

Очевидным является то, что сделать достоверный вывод об уровне устойчивости состояния всего рынка путем контроля единственного параметра нельзя. В силу некоторых частных условий ситуация на узком рынке (например, на рынке какао), контролируемая по одному показателю может существенно отличаться от устойчивости рынка в целом. Это означает, что нас должна интересовать задача многомерного контроля устойчивости (не когерентности) рынка по множеству параметров. Технически мы можем контролировать огромное количество параметров рынка, представленных, например, в форме текущего колебания цен на те или иные товары, фьючерсы, ценные бумаги, интегральные индексы активности (например, индекс S&P 500,

индекс Доу-Джонса, …). Только интегральных индексов активности существует более сотни, фьючерсов, ценных бумаг и товаров намного больше. Мы имеем дело с задачей очень большой размерности.

Формально, мы можем представить каждый из N контролируемых параметров рынка свой последовательностью i-тых отсчетов $v1_i$, $v2_i$, $v3_i$, …., vN_i. Рассчитать показатель Херста для каждого из контролируемых параметров не сложно. В простейшем случае, когда все контролируемые параметры независимы (отсутствуют корреляционные связи между параметрами), общая размерность системы составит сумму частных размерностей D1, D2, …., DN.

Для второго предельного случая, когда все контролируемые параметры сильно коррелированны $|r(v1, v2)| \approx 1$, $|r(v2, v3)| \approx 1, ..., |r(v1, vN)| \approx 1$, расчет общей размерности системы (общей энтропии) тривиален. Для сильно зависимых данных энтропия не увеличивается с ростом числа учитываемых параметров.

Для практики крайне важен промежуточный случай, когда модули коэффициентов парной корреляции анализируемых параметров находятся в интервале от 0.0 до 1.0. На данный момент оценка энтропии (числа степеней свободы системы) вполне возможна [38, 39] при условии одинаковой энтропии всех контролируемых параметров и их одинаковой по модулю коррелированности. Это означает, что мы, пользуясь номограммой связи высоко-размерной энтропии и коэффициента равной

корреляции, можем оценить суммарную энтропию (суммарную размерность) рынка как:

$$D_{\Sigma} \approx F(N, E(D), E(|r|)) \qquad (31),$$

где $E(D)$ - среднее значение фрактальной размерности по всем N контролируемым параметрам; $E(|r|)$ - среднее значение модулей парных корреляций между всеми N контролируемыми параметрами.

Тот факт, что мы не знаем реальной размерности рынка, особой роли не играет так как нам для оценки когерентности этот показатель не нужен. Если число учитываемых параметров N будет близко к реальной размерности рынка или превышать эту реальную размерность, мы будем иметь достаточно достоверные оценки когерентности. Выяснить какое значение суммарной энтропии для фиксированного списка из N контролируемых параметров является критичным можно путем экспертных оценок и предыдущего опыта. Если мы имеем след контролируемых параметров в момент очевидного кризиса, то вправе считать показатель фрактальной размерности в этот момент критическим (оценка снизу). Оценка допустимого значения фрактальной размерности с верху получается путем наблюдения локальных провалов размерности, из которых рынок выходит самостоятельно.

Таким образом, заимствуя методику расчета высоко-размерной энтропии из биометрии [38, 39], для рынка становится вполне возможно оценивать его текущую (динамическую) многомерную фрактальную размерность. При этом возникает естественный вопрос о допустимом временном интервале

наблюдения и допустимом числе отсчетов контролируемого параметра внутри этого допустимого интервала наблюдения. Как выбирать допустимый интервал наблюдения для рынка и необходимое число отсчетов в этом интервале является пока не решенным вопросом, но мы не будем останавливаться на нем, интуитивно опираясь на существование известной теоремы Котельникова. Это слишком глубокий вопрос, который пока не осознается в полной мере научно-экономической общественностью.

В дальнейших рассуждениях будем исходить из гипотезы о том, что дискретизация по времени потока контролируемых параметров рынка уже выбрана корректно и, при необходимости, может быть изменена. То есть, индекс Доу-Джонса, при необходимости, может рассчитываться не только на момент окончания рабочего дня, но и чаще. Нет технологических ограничений на то, чтобы вычислять частные индексы Доу-Джонса на момент окончания половины рабочего дня или даже на момент окончания каждого часа. Есть только предпосылки целесообразности этих вычислений, построенные на некотором аналоге теоремы Котельникова для рынков.

Предположим, что мы имеем поток корректных данных о состоянии контролируемого параметра рынка с интервалом в 1 час. Далее будем исходить из того, что рынок достаточно устойчив (не когерентен) и нам необходимо вычислять по каждому из контролируемых параметров свой показатель Херста. Весьма и весьма примитивные расчеты показывают, что 32 отсчетов (данных, собранные за полутора суточный интервал), 64 отсчетов

(трое суток), 128 отсчетов (неделя) для надежной оценки текущего значения показателя Хэрста недостаточно. Для надежной оценки показателя Херста необходимо как минимум от 2024 до 4096 отсчетов (от 8 до 16 раз больше данных), собираемых за один или два месяца. То есть, прямые процедуры вычисления показателя Херста (27), (28), (29) способны отслеживать только месячную и двухмесячную фрактальную размерность рынка. Возникает вопрос: можно ли сократить интервал наблюдения без существенной потери качества наблюдений до интервала в одну неделю?

Ответ на этот вопрос положительный и базируется он на том, что для вычисления автокорреляционной функции $r_{vv}(\tau)$ исследуемого временного ряда вполне достаточно 128 отсчетов. В этом отношении Мандельброт [40] не прав, рассматривая автокорреляционные функции как некоторое отображение только короткой памяти, а показатель Херста, как некоторый показатель долговременной памяти. Зная автокорреляционную функцию исследуемого процесса, мы можем по ней найти соответствующий показатель Херста [43].

Очевидно, что любой случайный процесс v(t), не являющийся «белым шумом», можно рассматривать как отклик некоторого линейного динамического звена с импульсной переходной функцией $w(\tau)$ на идеальный белый шум z(t):

$$v(t) = \int_0^T z(t) \cdot w(t-\tau) \cdot d\tau = z(t) \otimes w(t) \qquad (32),$$

где T – время «короткой» памяти линейного динамического звена,

$\otimes$ - операция свертки.

Если входное воздействие z(t) действительно является «белым шумом», то автокорреляционная функция исследуемого сигнала $r_{vv}(\tau)$ будет совпадать с автосверткой импульсной переходной функции:

$$r_{vv}(\tau) = \int_{-2T}^{+2T} w(\tau) \cdot w(\tau - t) \cdot dt = w(\tau) \otimes w(\tau) \qquad (33).$$

Решая интегральное уравнение (33) во временной или в частотной области [41, 42], мы всегда можем перейти от автокорреляционной функции $r_{vv}(\tau)$ к эквивалентной ей импульсной переходной функции $w(\tau)$.

В свою очередь, зная импульсную переходную функцию $w(\tau)$, мы можем воспользоваться генератором «белого шума» и создать последовательность z(t), далее вычислить ее свертку с импульсной переходной функцией (6). В конечном итоге мы получаем некоторую длинную последовательность данных (от 4096 отсчетов и выше), пригодную для корректного оценивания показателя Херста через применение формул (27), (28), (29). Таким образом, мы оказываемся способны оценивать показатель Херста на малых интервалах времени, представленных малым количеством отсчетов (от 32 отсчетов до 256 отсчетов).

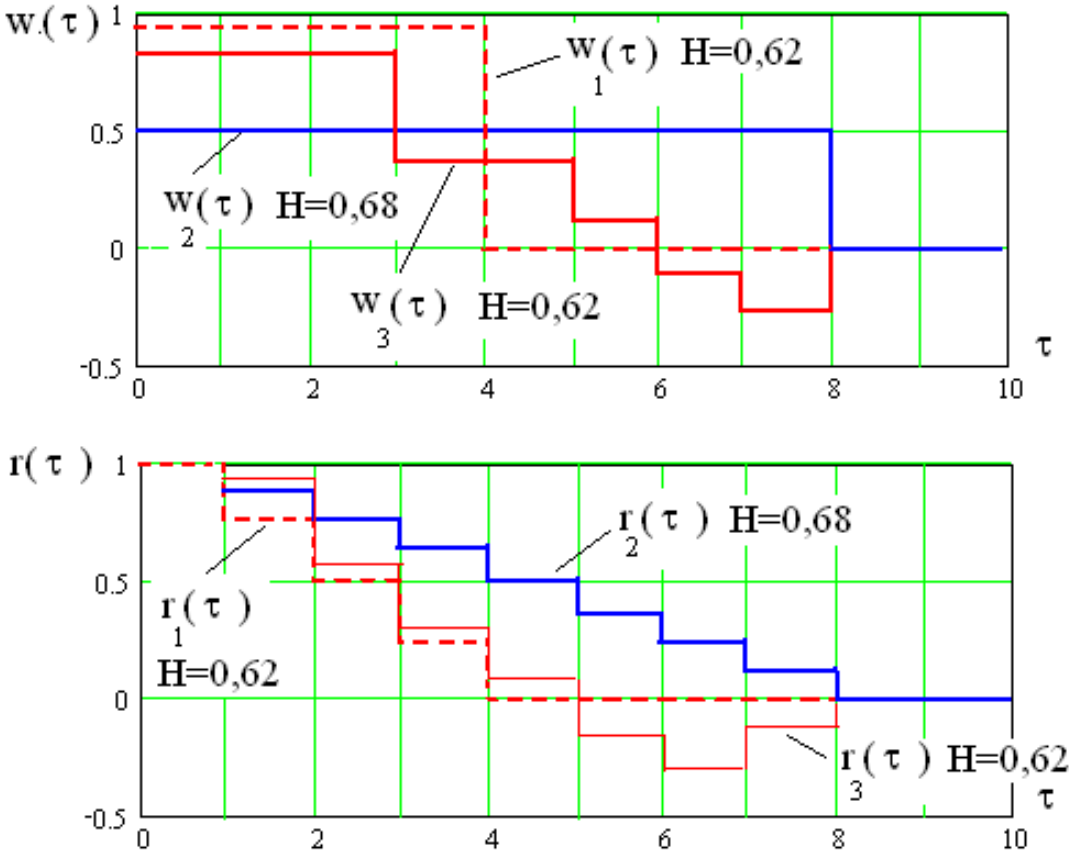


Рис. 30. Примеры разных импульсных переходных функций линейных звеньев, дающих одинаковое значение показателей Херста

Этот подход к ускорению процедур вычисления показателя Херста иллюстрируется рисунком 30, где отображены импульсные переходные функции трех разных линейных фильтров $w_1(\tau)$, $w_2(\tau)$, $w_3(\tau)$ и соответствующие им автокорреляционные функции не белого шума $r_1(\tau)$, $r_2(\tau)$, $r_3(\tau)$.

Первое и третье линейные звенья дают выходной случайный процесс с одинаковым значением показателя Хэрста H=0,62. Импульсные переходные функции $w_1(\tau)$, $w_3(\tau)$ специально подобраны таким образом, чтобы обеспечить выходной псевдостучайный процесс с одинаковым значением показателя Хэрста. Вторая импульсная переходная функция $w_2(\tau)$ является растянутой в два раза функцией $w_1(\tau)$. Она дает самый высокий

показатель Хэрста H=0,68.

Очевидно, что вычисление автокорреляционных функций того или иного случайного (псевдослучайного) процессов всегда будет осуществляться с большей точностью, чем соответствующий показатель Хэрста. Мы можем либо сократить объемы исходного статистического материала и вычислять показатель Хэрста на меньших выборках данных, либо существенно увеличить точность вычислений за счет предварительного оценивания автокорреляционной функции и восстановления по ней импульсной переходной функции.

19. Искусственные языки для программирования искусственного сознания и обучения искусственного подсознания

Сознание и подсознание интеллекта (искусственного и естественного) являются эффективными инструментами противостояния высокой энтропии окружающего нас информационного хаоса. Каков бы ни был уровень исходной неопределенности нужной для нас задачи, мы способны решить ее, принимая во внимание достаточно большое число влияющих параметров. Если задачу решить не удается, то мы учитываем недостаточное число переменных. Недостаток может появляться из-за ограниченности поля нашего зрения, слуха, чувств или чувствительности наших инструментов. Кроме того, недостаток может образовываться просто потому, что наши вычислительные возможности ограничены как во времени, так и в пространстве.

Опыт, полученный при проектировании и применении биометрического подсознания, показывает, что нейросетевой преобразователь биометрия-код должен свертывать входную неопределенность данных «Свой» практически до нуля. Существенно большая неопределенность образов «Чужие» наоборот усиливается нейросетевым подсознанием через хеширование до нескольких сот бит энтропии случайных кодов «Чужие». Получается, что по отношению к энтропии образов «Свой» и «Чужие» нейросетевые приложения биометрического подсознания ведут себя совершенно по разному. Энтропию образа «Свой» подсознание сжимает почти до нуля, а энтропию образов «Чужие» нейросетевое подсознание усиливает путем хеширования (перемешивания данных). При этом хеширование совершенно не обязательно следует выполнять на дискретном уровне, например, сложением по модулю два $\oplus$, расположенным в обратной связи блок-схемы рисунка 19. Если использовать двухслойные или трехслойные сети нейронов, то эффект хеширования данных «Чужие» также присутствует, хотя он становится не таким сильным.

Усиление энтропии или хеширование образов «Чужой» необходимо для борьбы с коллизиями образов «Свой» - «Чужой». Чем длиннее кодо-слово «Свой» в некотором искусственном языке биометрических приложений, тем менее вероятно возникновение в этом языке коллизий. Слова искусственного (естественного) языка имеют разную значимость (информативность), соответственно, они должны иметь и разную длину. Максимальная длина кодов слов языка искусственного сознательного интеллекта биометрических

приложений обусловлена обеспечиваемой этими приложениями уровнем информационной безопасности или вероятностью ошибок второго рода (возникновении случайной коллизии и ошибочного пропуска «Чужого» как «Своего»).

Так как мы научились создавать искусственное нейросетевое подсознание, мы должны научиться создавать искусственные языки, способные работать с новыми сущностями и их отображениями в виде кодов-слов нового языка. Ранее созданные формальные языки типа «Фортран» и «Паскаль» ориентированы исключительно на ручное написание программ мозгом человека-программиста и практически не имеют избыточности. Для того, чтобы написать программу на одном из старых полностью формализованных языков программирования требуется полная формализация задачи. Пока нет полностью отработанной блок-схемы формального решения задачи, нет смысла привлекать писателей-программистов, переводящих формализованную блок-схему в коды программы ее реализации.

Такой подход к программированию руками человека хорошо работал первые 50 лет эры электронных вычислительных машин, когда еще незапрограммированных, но формализованных или почти формализованных задач было достаточно много. Сегодня все формализации задач, созданные начиная со времен древнего Китая, уже переведены в программные коды и кем-то приватизированы. Появляется иная парадигма отказа от полной формализации задач, увеличения их размерности до необходимого, программирования нейросетевого подсознания через его обучение на примерах «Свой» и «Чужие». Основные

элементы этой новой технологии программирования через обучение уже отработаны и даже стандартизованы. Однако, языка для их объединения со старыми традиционными технологиями программирования пока нет.

Попытки решить проблему инженерии знаний с привлечением таких языков как «Пролог», «Лисп» ничего не дает, так как эти языки ориентированы только на низко-размерную логику сознательной части естественного или искусственного интеллекта. Мешает «бритва Оккама». Низко-размерными инструментами нельзя решать высоко-размерные задачи. Просто добавить к «Прологу» или «Лиспу» маленькие нейронные сети с малым числом входов нецелесообразно. К полноценной логике, выводов, доказательств, проверок уже имеющегося низко-размерного сознания искусственного интеллекта необходимо добавлять нейросетевое подсознание очень высоких (при необходимости как угодно больших) размерностей. Только в этом случае происходит качественный скачок интеллектуальности наших автоматов. При этом, мы поднимаемся с уровня ручного программирования на уровень автоматического синтеза программ, и Россия здесь лидер, так как мы имеем первый в мировой практике национальный стандарт по этой тематике [7]. Производительность автоматических синтезаторов подобных программ оказывается примерно в миллион раз выше, чем производительность программирования в ручном режиме (программы становятся почти бесплатными, так как исчезает ручной труд людей программистов).

Сдерживающим фактором развития новых технологий является отсутствие нового языка программирования, который с

одной стороны должен заимствовать жесткие конструкции традиционных языков программирования, а с другой стороны должен иметь возможность работы с высоко-размерным нейросетевым подсознанием приложений искусственного интеллекта. То есть, в новых языках «НейроПролог» или «БиоЛисп» должны появиться такие команды как: «Создать сеть нейронов», «объявить выходное кодо-слово нейросети», «обучить сеть нейронов», «тестировать сеть нейронов», «взаимно упорядочить нейросети по расстоянию Хэмминга их нечетких кодо-слов»,… Предположительно, следующее поколение языков одновременного программирования сознания искусственного интеллекта и подсознания искусственного интеллекта будет иметь значительную избыточность и, соответственно, будет много ближе к естественным языкам общения людей.

20. Отрицательная информация или дезинформация

То, что информация может быть разнополярна, отмечалось еще Бриллюэном [1]. В интерпретации Шеннона информация всегда положительна только из-за того, что он рассматривает только информационное измерение объема контейнера со знаниями в виде текста на том или ином языке людей. Если мы будем, как основу, рассматривать некоторый активный субъект (это может быть как человек, так и машина), у которого есть цель, то мы можем заранее указать некоторую априорную вероятность – P_0 выполнения субъектом свой задачи.

У субъекта есть собственная программа его действий - χ_0, достигающая поставленной цели с вероятностью P_0. При этом

субъект выполняет свою программу, пользуясь поступающей к нему из вне информацией, например, в виде понимаемых текстов. Длина текста не имеет значения, важно только его содержание. Фактически, субъект способен извлечь знание (извлечь смысловую информацию), которую он добавляет в свою собственную программу действий. При этом мы получаем другую программу достижения цели χ_1, которая достигает цели с вероятностью – P_1. Если оказывается, что вероятность достижения цели выросла, то смысловая информация положительна.

Сама процедура вычисления информации остается традиционной: $$I = -\log_2(\frac{P_0}{P_1}) \qquad (34).$$

Если оказывается, что вероятность достижения цели снизилась, то полученная смысловая информация отрицательна (мы имеем дело с обманом или дезинформацией субъекта). Хорошей иллюстрацией этого положения является вероятность всхожести семян. Если семена правильно хранились, то их всхожесть может составлять до 98%. Семена начинают прорастать, попадая в теплую и влажную среду. Тепло и высокая влажность запускают механизм прорастания, однако последующий заморозок может убить 99% всходов. В этом случае информация полученная семенами о раннем тепле будет ложной (отрицательной информацией или дезинформацией), которую можно рассчитать по формуле (33).

В природе ряд растений имеет защиту от такой отрицательной информации. Часть семян таких растений всходят с задержкой на

несколько сезонов. У некоторых растений часть семян начинает обладать всхожестью только после лесного пожара (кратковременного нагрева до высокой температуры).

Только активные субъекты, имеющие цель и программу ее достижения и способные к самопрограммированию и саморазвитию, могут быть обмануты. Только для них целесообразно вводить понятие отрицательной информации или дезинформации. В этом контексте затронутая тематика может показаться преждевременной, однако, это не так. Мы сами являемся самообучающимися существами и стоим на пороге массового применения самообучающихся автоматов. В России введен первый стандарт [7], регламентирующий требования автоматическому самообучению нейронных сетей. Соответственно, мы уже имеем технологии самообучения, и исследование приемов дезинформации самообучающихся автоматов будет весьма и весьма востребовано.

Информационное общество можно называть и обществом «обмана» или обществом «дезинформации», объемы дезинформации постоянно растут. Спам и иная реклама - это почти полная дезинформация. В интернете и СМИ объемы положительной информации снижаются, а объемы дезинформации увеличиваются. При этом, никто не виноват. Производители пива просто оплачивают рекламу, телевизионщики ее просто крутят и получают свой процент от обмана нас всех этой самой рекламой. Все вроде бы законно, однако происходит смещение статистик окружающей нас действительности, это мы чувствуем, но не осознаем. Нас обманывают рекламой на уровне подсознания.

Рекламы пива и водки в СМИ должно быть ровно столько, сколько среднестатистический человек пьет их в жизни. Если пропорции нарушены, нас обманывают, нас дезинформируют, на нас наживаются СМИ и производители алкоголя, для которых лучший вариант, когда все мы станем алкоголиками.

Если с экрана постоянно льется кровь и насилие, нас опять обманывают, искажают действительность в нужную правоохранителям сторону. Они так оправдывают свой хлеб. Даже небольшие статистические смещения множества все «Чужие» сильно меняют самооценку «Я». Это очень опасно и проверить это очень трудно. Искажать действительность никакие СМИ не имеют права, необходимо научиться измерять объемы общественной и личной дезинформации и вводить технические регламенты по ее ограничению.

Если вчера мы знали, что в пельменях есть мясо, то сегодня можно быть уверенным только в том, что там есть реклама и налоги. Есть ли там мясо неизвестно, это новый информационный мир. Обманывать нас всех вместе стало очень просто, тот кто обманывает по крупному, имеет гарантированную защиту (крупный бизнес защищают адвокаты, правоохранители, государство). В СССР было мало пельменей, но в них было мясо. То, что продают сейчас пельменями не является, за этот обман никто не несет ответственности. Государство самоустранилось и разрешает нас всех обманывать, чем дальше, тем будет хуже. Создается впечатление, что информационное общество - это общество навязываемого нам всем обмана. Должна быть обратная ситуация. Информационное государство должно защищать нас от

дезинформации СМИ и корпораций.

21. Континуально-дискретные ускорители мышления и точных многомерных вычислений

Нас всех удивляет то, что мы способны очень быстро решать задачи огромной размерности (огромной вычислительной сложности). В литературе это объясняют высоким параллелизмом нейросетевых вычислений, но это далеко не так. Тактовая частота наших мозгов всего 100 Герц, простым распараллеливанием вычислений нельзя ничего объяснить.

Гораздо более рациональным является объяснение наших удивительных интеллектуальных возможностей наличием некоторых фазовых ускорителей (уточнителей) вычислений или мышления, что отображено на рисунке 30.

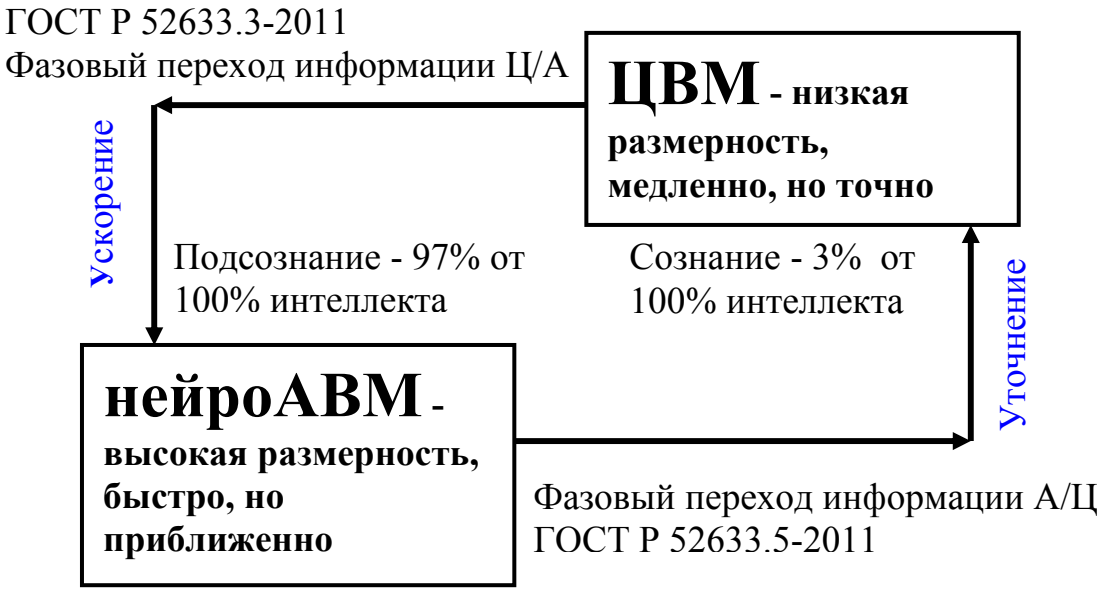


Рис. 30 Ускоряюще-уточняющая петля из прямого и обратного многомерных фазовых переходов двух состояний информации

Аналоговые вычислительные машины (АВМ) обладают огромной скоростью вычислений, но имеют низкую точность.

Цифровые вычислительные машины (ЦВМ) медленные, но очень точные. Похоже, что на стыках аналог-цифра и цифра-аналог можно организовывать эффективные ускорители и уточнители вычислений.

Ранее все АВМ были специализированными (не универсальными), но сегодня этот недостаток снят стандартом ГОСТ Р 52633.5 [7]. Руководствуясь этим стандартом можно автоматически настраивать АВМ (нейросеть) на любую задачу, имея не более 20 примеров ее решения. Более того, обученная АВМ (нейросеть) уже имеет готовый стык с ЦВМ, так как дает выходные коды. Сама нейросеть (АВМ) остается быстрой, но низко точной (ошибочный пропуск «Чужого» в каждом разряде возникает с вероятностью 0.5). Однако 256 нейронных сетей уже практически не ошибаются из-за того, что совместная обработка (сравнение с эталоном) осуществляется ЦВМ.

По аналогии с физикой состояний обычного вещества (жидкое/газообразное) в математике существуют фазовые переходы представления информации в форме многомерных континуумов и в цифровой форме. Эти переходы можно использовать для очень эффективного уточнения, изначально неточных аналоговых решений. Алгоритмы обучения нейронных сетей по ГОСТ Р 52633.5 [7] позволяют поднять точность принятия решений в миллиарда раз (раздел 11, формула (17а)) по сравнению с точностью решения одного нейрона.

Следует отметить, что наличие только одного перехода по уточнению решений еще не может объяснить способностей нашего интеллекта. Наш интеллект, видимо, способен использовать еще и

второй фазовый переход цифра-аналог, приводящий к гигантским ускорениям вычислений.

Ускорение, получаемое на обратном фазовом переходе информации цифра-аналог пока ограничивается процедурами, рекомендуемыми ГОСТ Р 52633.3 [10]. Эффект от ускорения вычислений подробно описан в разделе 16 данной работы. Сравнительные результаты ускорения вычислений энтропии текстов в зависимости от числа знаков в исследуемой группе даны в следующей таблице.

Таблица времени вычисления энтропии текстов на обычной ЦВМ без аналоговых ускорителей.

Число букв (знаков) в группе	Вычисление энтропии по Шеннону		Предсказание энтропии по Хэммингу	
	Достаточный размер текстовой выборки	Время вычислений	Достаточный размер текстовой выборки	Время вычислений
1 знак	1 000 знаков	0.1 секунды	1 001 знаков	0.1 секунды
2 знака	33 000 знаков	3.3 секунды	1 002 знаков	0.2 секунды
3 знака	1 000 000 знаков	100 секунд	1 003 знаков	0.3 секунды
4 знака	33 млн. знаков	55 минут	1 004 знаков	0.4 секунды
5 знаков	$1*10^9$ знаков	33 часа	1 005 знаков	0.5 секунды
6 знаков	$33*10^9$ знаков	40 суток.	1 006 знаков	0.6 секунды
7 знаков	$1*10^{12}$ знаков	3.6 лет	1 007 знаков	0.7 секунды
8 знаков	$33*10^{12}$ знаков	120 лет	1 008 знаков	0.8 секунды
9 знаков	$1*10^{15}$ знаков	3800 лет	1 009 знаков	0.9 секунды
16 знаков	10^{22} знаков	больше возраста Земли	1 016 знаков	1.6 секунды
32 знака	10^{47} знаков	::::::::::::::::	1 032 знаков	3.2 секунды
64 знака	::::::::::::::::::::	::::::::::::::::::	1 064 знаков	6.4 секунды

Из таблицы следует, что уже для группы из 9 знаков обычный алгоритм на обычной ЦВМ требует затрат в 3800 лет машинного времени. Для групп из 32 и 64 знаков вычисления на обычной ЦВМ потребуют времени больше, чем время жизни Вселенной. В то же время ускоритель Хэмминга, написанный для обычной ЦВМ, позволяет делать все вычисления за несколько секунд. Это происходит из-за того, что после вычисления дискретных статистик

Хэмминга производится переход к аналоговой форме расчетов (вычисляется интеграл (26) стр. 88). Ускорение в миллиарды лет дает именно скачек из дискретных статистик Хэмминга к аналоговому (непрерывному) представлению информации в форме нормального закона распределения.

Таким образом, использование прямого фазового перехода А/Ц позволяет поднять точность решений в миллиарды раза, а использование обратного фазового перехода Ц/А позволяет получать ускорение вычислений в миллиарды раз. Видимо, наш интеллект с его огромными возможностями постоянно использует многократные ускорения и уточнения вычислений на фазовых переходах информации А/Ц и Ц/А. Мы циклически думаем на наших языках [44] и, соответственно, наши языки построены на многократных итерационных переходах уточнений А/Ц и ускорений мышления Ц/А. Только в этом случае нас перестает волновать низкая тактовая частота аналого-цифрового процессора в наших головах. Также в рамках этих представлений легко объяснить основной постулат Хомского [44]. Учить первый родной язык много проще, чем переучиваться на другой второй язык. Из-за высоких затрат на обучение первому языку существует подсознательный запрет на избыточное дополнительное переобучение на второй язык.

Сколько бы мы ни поднимали частоту цифровой части вычислительных машин в головах у роботов, умнее они не станут, так как у них нет мощного высоко-размерного аналогово-нейросетевого (мгновенного) подсознания. Наши машины-роботы действительно могут стать разумными только если их интеллект будет организован так же, как интеллект людей. То есть, 97% ресурсов должно отдаваться мгновенному аналогово-

нейросетевому подсознанию и только 3% должен потреблять цифровой процессор сознания (рис. 31). Огромные вычислительные возможности таких структур строятся на многократных фазовых переходах во время мышления. Отрыв мгновенного аналогово-нейросетевого подсознания от медленного цифрового сознания и их раздельное исследование ничего не дает. Такая декомпозиция убивает главное в процессах мышления их совокупную быстроту и точность, получаемые через цикличность (итеративность).

Так же как в 19 веке технологический рывок человечеством был получен на фазовом переходе вода-пар (появились паровозы), технологический рывок в 21 века по интеллектуализации наших машин может быть получен только на многократных физико-математических фазовых переходах представления информации аналог-цифра и цифра-аналог. Квантовые компьютеры [45] пока еще не созданы, более того в них нет особой необходимости. Фантастические ускорения вычислений получаются и без них. Вполне достаточно сцепить в петлю (рисунок 30) хорошо изученные и давно имеющиеся у нас аналоговые и цифровые вычислительные машины.

ЛИТЕРАТУРА:

1. Бриллюэн Л. Наука и теория информации. М.: ФизМатЛит, 1960 г.
2. Кульбак С. Теория информации и статистика. М.: Наука, 1967 г.
3. Яглом А.М., Яглом И.М. Вероятность и информация. М.: ДомКниги, 2007 г., 512 с.
4. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Изд-во Пензенского государственного университета, 2000 г. – 188 с.
5. Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности. Книга 15, серии «Нейрокомпьютеры и их применение» М.: Радиотехника 2004 г., 144 с.
6. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза-2005 г.

Издательство Пензенского государственного университета, 273 с.
7. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».
8. Саймон Хайкин Нейронные сети: полный курс. М.: «Вильямс», 2006. — С. 1104
9. Малыгин А.Ю., Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы тестирования нейросетевых механизмов биометрико-криптографической защиты информации /Пенза-2006 г., Издательство Пензенского государственного университета, 161 с.
10. ГОСТ Р 52633.3-2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора».
11. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / пер. с англ. В. Б. Афанасьева. — М.: Техносфера, 2006. — 320 с.
12. Гельфанд И.М. Лекции по линейной алгебре. М. 1998 г.
13. Боос В. Лекции по математике. Том 3: Линейная алгебра. М.: URSS/Книжный дом «ЛИБЕРКОМ», 2011.
14. Тихонов А.Н., Арсенин В.Я. Методы решения некорректных задач. М.: Наука, 1979, 248 с.
15. Лоусен Ч., Хенсон Р. Численное решение задач методом наименьших квадратов. – М.: Наука, 1966, 230 с.
16. Райс Дж. Матричные вычисления и математическое обеспечение. – М.: Мир, 1984 г. 412 с.
17. Иванов А.И. Ортогонализация алгоритмов быстрого обучения искусственных нейронных сетей большой и сверхбольшой размерности «Нейрокомпьютеры: разработка, применение» №6, 2009 с.11-13.
18. Язов Ю.К. и др. «Нейросетевая защита персональных биометрических данных» Книга 1 серии «Нейросетевая биометрия» //Ю.К. Язов (автор и редактор), В.И. Волчихин, И.Г. Назаров, В.А. Фунтиков, А.И. Иванов // М.: «Радиотехника» 2012 г., 210 с.
19. ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
20. Фунтиков В.А., Назаров И.Г., Бурушкин А.А. Национальные стандарты России: конфиденциальность персональных биометрических данных. «Стандарты и качество» № 7, 2010 г. с. 28-33.
21. Иванов А.И., Фунтиков В.А., Ефимов О.В. Описание к патенту RU 2346397 «Способ защиты персональных данных биометрической идентификации и аутентификации», приоритет от 26.06.07.
22. ГОСТ Р 52633.1-2009 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации».
23. ГОСТ Р 52633.2-2010 «Защита информации. Техника защиты

информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации».
24. Андреев Д.Ю., Иванов А.И., Захаров О.С., Хозин Ю.В. Модификация меры Хемминга через взвешивание мерой стабильности выходных данных нейросетевых преобразователей биометрия-код. «Нейрокомпьютеры: разработка, применение» №6, 2009 с. 49 - 52
25. Рутковская Д., Пилинский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы— М: Горячая линия-Телеком, 2008. — С. 452.
26. Емельянов В. В., Курейчик В. В., Курейчик В. М. Теория и практика эволюционного моделирования. — М: ФизМатЛит, 2003. — С. 432.
27. Брюс Шнайер Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 816 с.
28. Cover T.M. and R.C. Ring "A Convergent Gambling Estimate of the Entropy of English", IEEE Transactions on Information Theory v. IT-24, n. 4 Jul 1978, pp. 413-421.
29. Иванов А.И., Фунтиков В.А., Майоров А.В., Надеев Д.Н. Моделирование кодовых последовательностей с энтропией естественных и искусственных биометрических языков. Инфокоммуникационные технологии, том 8, № 4, 2010 г., с. 75-79
30. Рыболовлев А.А., Рыжков А. П., Иванов А.И., Хальметова А.Н., Захаров О.С. Нейросетевой вокодер-архиватор, сохраняющий биометрические особенности голоса говорящего при высоком уровне сжатия шипящих звуков. «Нейрокомпьютеры, разработка и применение» № 3, 2012 г.
31. Елфимов А.В., Воячек С.А., Качайкин Е.И., Куликов С.В. Обучение нейросетевого идентификатора авторства рукописных текстов. «Нейрокомпьютеры: разработка, применение» №6, 2009 с. 17-21
32. ГОСТ Р 51061-97 «Системы низкоскоростной передачи речи по цифровым каналам. Параметры качества речи и методы измерений.»
33. Боос В. Лекции по математике. Том 4. Вероятность. Информация. Статистика. М.: URSS/Издательство ЛКИ, 2008 г., -216 с.
34. Петерс Э. Хаос и порядок на рынках капитала. Новый аналитический взгляд на циклы, цены и изменчивость рынка. М.: Мир, 2000 г., 333 с.
35. Мандельброт Б., Ричард Л.Х. (Не) послушные рынки: фрактальная революция в финансах. М.: «Вильямс», 2006 г., 400 с.
36. Vaga T. "The Coherent Market Hypothesis", Financial Analysts Journal, December/January 1991.
37. Callan E., Shapiro D. "A Theory of Social Imitation" Physics Today 27, 1974.
38. Фунтиков В.А., Надеев Д.Н., Иванов А.И. Связь энтропии выходных состояний нейросетевых преобразователей биометрия-код с коэффициентами парной корреляции. «Нейрокомпьютеры: разработка, применение» № 3 2012 г.
39. Фунтиков В.А., Надеев Д.Н., Иванов А.И. Оценка энтропии множества датчиков с учетом коррелированности их данных. «Датчики и системы» № 11, 2011 г. с. 3-6.

40. Mandelbrot B. “Statistical Methodology for Non-Periodic Cycles: From the Covariance to R/S Analysis”, Annals of Economic Social Measurement 1, 1972 г.
41. Эйкхофф П. Основы идентификации систем управления. М.: Мир. 1975- 517 с.
42. Льюнг Л. Идентификация систем. Теория для пользователя. М.: Наука, 1991 г., 432 с.
43. Иванов А.И., Егорова Ю.Ю. Корреляционный метод быстрой оценки текущего значения показателя Херста биометрических данных и данных рынка. «Нейрокомпьютеры: разработка, применение» №3, 2012
44. Хомский Н. Язык и мышление. М.: Издательство МГУ, 1972 г.
45. Китаев А., Шень А., Вялый М. Классические и квантовые вычисления М.: МЦНМО ЧеРо 1999 г., 190 с.

Словарь языка специальных терминов

Искусственный нейрон: сумматор с выходным пороговым нелинейным элементом, имеющим два состояния «0» и «1». Нейрон осуществляет преобразование непрерывных входных данных в два дискретных выходных состояния нелинейного элемента. Обучение нейрона ведут подбором весовых коэффициентов сумматора.

Нейросеть: совокупность нейронов, обрабатывающих множество входных непрерывных состояний биометрических или иных параметров, преобразуя их в выходной код, соответствующий коду слова некоторого языка. Различают сеть из одного, двух и более слоев нейронов.

Обучение нейрона: подбор весовых коэффициентов нейрона с тем, чтобы его отклик на примеры образа «Свой» с высокой вероятностью соответствовал заранее заданному состоянию выходной нелинейности, а образы «Чужой» давали другое состояние выходного нелинейного элемента с вероятностью 0.5 и выше.

Обучение нейросети: обучение совокупности нейронов таким образом, чтобы образ «Свой» давал на выходе нейронов код личного ключа «Свой» (название объекта), а образы «Чужой»

давали случайный выходной код. Желательно иметь алгоритм обучения с линейной вычислительной сложностью, тогда удается обучать нейронные сети с очень большой входной размерностью. Случайный перебор возможных состояний настроек сети имеет экспоненциальную вычислительную сложность и обучает большие нейронные сети бесконечно долго.

Тестирование нейрона: проведение проверки качества обучения на примерах образа «Свой», не использованных при обучении, и примерах образов «Чужие», также не использованных при обучении.

Информация: знания, предназначенные для понимания (использования) человеком или машиной, записанные на языке, доступном для понимания (использования) информации человеком или машиной. Зашифрованные данные являются информацией только для обладающего ключом расшифровывания.

Данные: последовательность непрерывных или оцифрованных значений какого либо параметра, наблюдаемых в окружающем мире (канале связи объектов окружающего мира).

Знания: умение, что либо выполнять, умение, что либо предсказывать. Знания могут быть высоко-размерными и низко-размерными. Выразить на языке можно только низко-размерные знания.

Формализованные знания: низко-размерные знания, выраженные на языке, на котором человек думает, говорит, слушает.

Не формализованные знания: высоко-размерные знания, которыми человек может воспользоваться на интуитивном (подсознательном уровне), но не может эти знания передать другим людям из-за отсутствия соответствующих понятий в языке общения и из-за относительно низкой размерности существующих языков.

Сознание: часть естественного интеллекта (искусственного интеллекта) работающая с высоко формализованными знаниями, выраженными на языке общения и понимания людей, а также понимаемые человеком программы искусственного интеллекта машин.

Подсознание: часть естественного интеллекта людей или искусственного интеллекта машин, отвечающая за решение задач очень высокой размерности и в том числе за перевод непрерывной высоко-размерной действительности в низко-размерные кодо-слова языка.

Язык: дискретное пространство кодов-слов, предназначенное для кодировки знаний при их передаче, хранении в памяти, осмыслении. Каждый язык обладает грамматикой совместного использования кодов слов и предназначен для связи сознания и подсознания.

Образ «Свой»: совокупность континуума примеров отображающего возможные состояния образа, выделяемого из окружающей действительности. Для биометрических нейросетевых приложений достаточно 20 примеров образа «Свой» для обучения его распознаванию.

Образ «Чужой»: образ одного из объектов, которые нас интересуют только как фон, на котором необходимо надежно выделить образ «Свой».

Образы «Чужие»: все образы «Чужой», которые могут быть представлены примерно сотней случайно выбранных образов «Чужой».

Пример образа «Свой»: примеры образа «Свой», используемые для обучения и/или тестирования нейронов подсознания.

Образы-родители: два образа «Чужой», которые могут быть использованы для получения образов потомков морфингом параметров образов-родителей «Чужой».

Образы-потомки: синтетические образы, полученные из образов-родителей. Обычно число образов потомков выбирают большим для образов-родителей с большим расстоянием Хэмминга между кодами-откликами нейронной сети, обученной распознавать один из образов-родителей.

Биометрический параметр: параметр биометрического образа, используемый для его распознавания, например, коэффициенты ряда Фурье для кривых колебания пера, возникающих при воспроизведении человеком рукописных букв.

Морфинг биометрических параметров: линейное взвешенное суммирование биометрических параметров двух образов-родителей.

Мутация биометрического параметра: случайное изменение одного или нескольких биометрических параметров.

Хеширование данных: перемешивание данных путем использования любых нелинейных преобразований. Различают простое хеширование и криптографическое хеширование. Криптографическое хеширование считается идеальным (гарантированно необратимым).

Нейросетевой функционал: функционал, который преобразует совокупность непрерывных входных данных нейронов в его дискретные выходные состояния. Наиболее часто используются нейроны с двумя выходными состояниями «0» и «1», однако число состояний может быть любым (зависит от вида выходной нелинейности нейронов).

Матрица нейросетевых функционалов: матрица, каждый элемент которой является некоторым нейросетевым функционалом. При умножении вектора входных непрерывных параметров на матрицу нейросетевых функционалов получается слово выходного кода, принадлежащее некоторому языку формализации действительности.