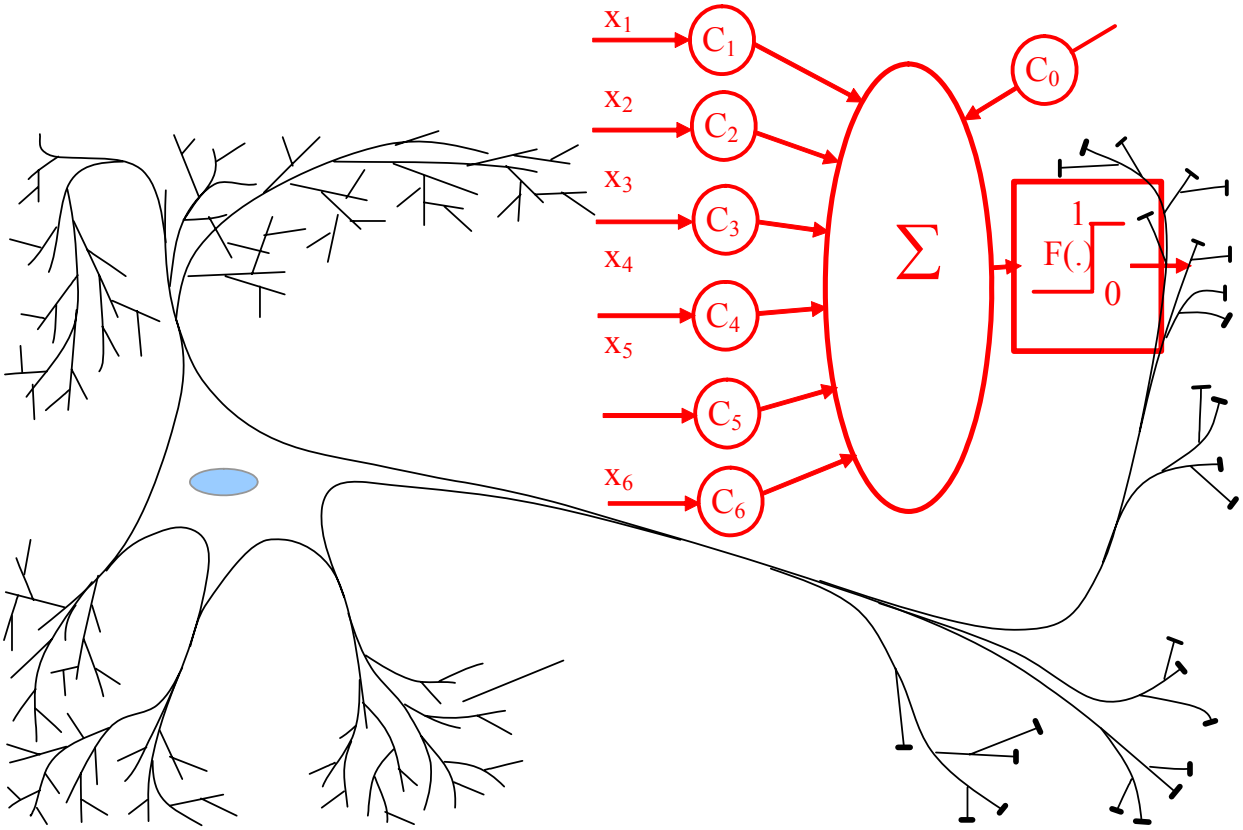
Иванов А.И.

# АВТОМАТИЧЕСКОЕ ОБУЧЕНИЕ БОЛЬШИХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ В БИОМЕТРИЧЕСКИХ ПРИЛОЖЕНИЯХ

Учебное пособие к пакету лабораторных работ, выполняемых в среде моделирования "БиоНейроАвтограф" (http://пниэи.рф/activity/science/noc.htm)




Пенза – 2013 г.

УДК: 004.8; 681.3

Электронная книга издательства ОАО "Пензенский научно-исследовательский электротехнический институт"

Рецензенты:
– доктор технических наук, профессор, начальник управления ФАУ "ГНИИИ ПТЗИ ФСТЭК России" (г. Воронеж) Язов Ю.К.;
– доктор технических наук, профессор филиала Военной академии связи им. С.М. Буденного (г. Краснодар) Финько О.А.

## РЕФЕРАТ

Иванов А.И. **Автоматическое обучение больших искусственных нейронных сетей в биометрических приложениях.** Пенза-2013 г.

Учебное пособие помогает освоить основы автоматического обучения больших искусственных нейронных сетей, использующихся в биометрических приложениях. Дан общий обзор проблем, связанных с быстрым автоматическим обучением нейронных сетей по ГОСТ Р 52633.5 и их тестированием по ГОСТ Р 52633.3. Пособие построено в форме комментариев к лабораторным работам, которые выполняются в среде моделирования "БиоНейроАвтограф", бесплатно предоставляемой учебным заведениям Белоруссии, России, Казахстана. Изложение материала ведётся в общедоступной форме, ориентированной на уровень знаний студентов, изучающих искусственные нейронные сети самостоятельно или в рамках какого-либо университетского курса.

## Введение

В настоящее время происходит исторический переход от капиталистического индустриального общества к информационному, постиндустриальному обществу. В отличие от всех предыдущих исторических формаций (матриархат, рабовладение, феодализм, капитализм) информационное общество строится на приватизации информации и её оценивании. Любая информация оценивается (начинает иметь свою цену), может продаваться или выступать в роли активов. Информационная свобода в новом обществе определяется тем, насколько свободно человек может получать и отдавать информацию в открытом информационном пространстве. Сложность проблемы обеспечения информационной свободы обусловлена тем, что наряду с оборотом достоверной информации общество знаний будет иметь весьма и весьма ощутимый оборот недостоверной информации (дезинформации).

В отличие от информации, дезинформация ничего не стоит, точнее она имеет отрицательную стоимость. Человек не хочет получать дезинформацию и пытается всячески защититься от неё, дезинформатор, напротив, пытается всячески навязывать свою дезинформацию тем, кого он обманывает. Спам и реклама – это примеры дезинформации, имеющей отрицательную стоимость. Именно по этой причине рекламу стараются совместить с полезной информацией, иначе её никто не увидит.

Самым эффективным способом дезинформации является подмена личности. Неприятность в том, что сегодня безопасность сети Интернет построена на паролях. Пароли надежны только тогда, когда они длинные и случайные, однако люди не хотят и не могут запоминать длинные случайные пароли или личные криптографические ключи. Получается тупик. С одной стороны мы можем использовать криптографию и с помощью неё можем защитить целостность информации или её конфиденциальность, но с другой стороны, мы должны где-то хранить личные криптографические ключи. Обычному человеку негде хранить свой личный криптографический ключ, используемый, например, для формирования электронной цифровой подписи.

Цифровой капкан электронной подписи состоит в том, что производители криптографических средств её формирования предоставляют пользователю контейнер с его личным криптографическим ключом, который защищён обычным паролем. Стойкость криптографического ключа на этапе технической реализации подменяется стойкостью обычного пароля. Любой, скопировавший "Чужой" контейнер с "Чужим" личным ключом может стать эффективным дезинформатором и подписывать "Чужие" электронные документы "Чужой" электронной подписью, так как подобрать "Чужой" пароль не очень сложно. В итоге обычный человек, рискнувший воспользоваться криптографическим механизмом электронной цифровой подписи, получает дополнительный риск попасть в электронно-цифровое рабство к кому-то из дезинформаторов (электронно-цифровому преступнику).

Защититься от угрозы электронно-цифрового рабства можно только одним путем: нужно усиливать парольную и криптографическую защиту. Проще всего это можно сделать через биометрию, например, можно научить сеть искусственных нейронов преобразовывать образ человека в его пароль или криптографический ключ. Если создавать биометрическую поддержку для асимметричной криптографии, то необходимо иметь технологию нейросетевого связывания открытых биометрических образов человека (автографа, рисунка отпечатка пальца, рисунка радужной оболочки глаза, …) с открытым криптографическим ключом. Личный (секретный) криптографический ключ необходимо связывать с тайным биометрическим образом человека (рукописным паролём, голосовым паролём). Эта ситуация иллюстрируется рисунком 1.


Рис. 1. Нейросетевое связывание открытых (общедоступных) биометрических образов человека с его открытым ключом и связывание тайных биометрических образов человека с его закрытым ключом.

Принципиально важным моментом технологии является то, что из параметров обученной искусственной нейронной сети нельзя извлечь информацию о секретном ключе пользователя и о его тайном биометрическом образе. Именно это позволяет обычным людям безопасно хранить в нейросетевых контейнерах свои персональные биометрические и криптографические данные. Образно говоря, извлечение искусственных мозгов из программного биометрического автомата ничего не дает злоумышленнику. Он не может воспользоваться "Чужими" знаниями, размещенными в "Чужом" нейросетевом контейнере. Понять о чём думал или будет думать нейросетевой искусственный интеллект биометрической защиты злоумышленник не может.

Следует подчеркнуть, что защита информации криптографическая и биометрическая – это лицензируемые виды деятельности. Этой работой не может заниматься кто угодно, продаваемые на национальном рынке биометрические и криптографические продукты должны иметь соответствующие сертификаты. Биометрия и криптография – это весьма и весьма важные информационные технологии и каждое информационно-сильное государство стремится иметь собственные национальные стандарты, регламентирующие требования к таким информационным продуктам. Создавать собственные национальные стандарты – это очень дорогое удовольствие, на сегодня позволить себе это удовольствие могут только два государства США и Россия.

Исторически сложилось так, что США является безусловным лидером по созданию национальных стандартов, регламентирующих полицейскую биометрию, в частности биометрию международных паспортов. С начала 90-х годов прошлого века по настоящий момент (апрель 2013 года) в США было создано порядка 100 национальных биометрических стандартов. Позднее (с 2002 года по настоящее время) примерно половина национальных биометрических стандартов США были переведены в ранг международных биометрических стандартов усилиями специально созданного для этой цели технического комитета ISO/IEC JTC1 SC37 (Biometrics).

В России все складывалось совершенно иначе. В 90-х годах прошлого века развал Российского государства не позволил нашей стране полноценно участвовать в международных усилиях по стандартизации. Однако уже в самом начале 21 века положение изменилось и, начиная с середины нулевых годов, Россия активно создает собственные национальные стандарты, регламентирующие требования к биометрическому усилению парольной и криптографической защиты. В этом отношении усилия России дополняют усилия США и других, развитых в информационном

отношении, стран. Однако на данный момент Россия всё же остается единственной страной целенаправленно создающей фундамент информационной безопасности своего будущего через объединение отечественной биометрии и отечественной криптографии. Кооперация международных усилий по биометрической стандартизации отражена на рисунке 2.

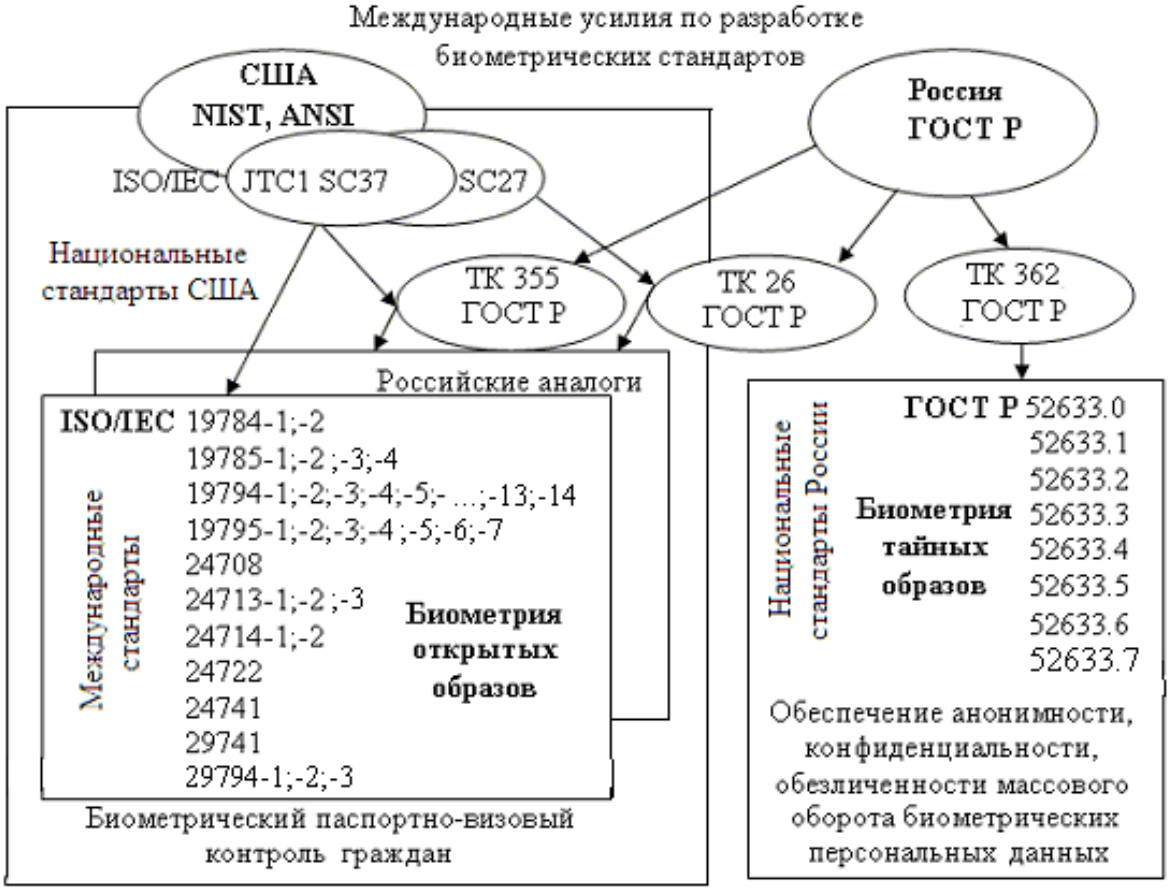



Рис. 2. Усилия России и США по созданию двух, дополняющих друг друга ветвей биометрических стандартов

Средства биометрико-нейросетевой защиты персональной информации очень быстро развиваются и нуждаются в создании специальных учебных пособий и лабораторных работ. Материал, изложенный в национальных стандартах серии ГОСТ Р 52633-20xx, на данный момент доступен пониманию только для узких специалистов очень высокой квалификации, имеющих собственный опыт разработки биометрических приложений. В связи с этим предпринята попытка изложить основные моменты пакета национальных стандартов в максимально упрощенной форме, доступной рядовому студенту, не имеющему собственного опыта обучения искусственных нейронных сетей и не имеющего собственного опыта разработки биометрических приложений. Предполагается, что студент очень быстро приобретет свой личный положительный опыт, выполнив одиннадцать лабораторных работ в среде моделирования "БиоНейроАвтограф". В данном учебном пособии в очень компактной форме даны основные положения теории, которые должны подтверждаться практикой при выполнении обучающимися простейших и интуитивно понятных лабораторных работ.

# 1. Общие положения обучения искусственных нейронных сетей

## 1.1. Устойчивость обучения одного нейрона

Искусственный нейрон строится как модель естественных нейронов, имеющихся у животных и людей. Функция нейрона – это принятие им некоторого простейшего решения в результате учёта состояний нескольких входных параметров. Все искусственные нейроны состоят из входных данных, сумматора и выходного нелинейного элемента (смотри рисунок 3). Простейший нейрон имеет пороговый нелинейный элемент, дающий на выходе два состояния "0" или "1". В данном пособии будут рассматриваться только нейронные сети, состоящие из простейших нейронов с пороговыми элементами, которые обучаются и тестируются в программной среде моделирования "БиоНейроАвтограф".

Нейроны и сети из нейронов могут решать множество совершенно разных прикладных задач. Среда моделирования "БиоНейроАвтограф" создана для решения задачи преобразования динамики рукописного пароля в код длинного пароля или ключа доступа. При воспроизведении рукописного пароля перо совершает движение по двум координатам X(t), Y(t). Далее кривые колебаний пера или кривые движения манипулятора "мышь" X(t), Y(t) раскладываются в двухмерный ряд Фурье, а уже коэффициенты двухмерного ряда Фурье рассматриваются как контролируемые биометрические параметры. Преобразование биометрических данных в биометрические параметры для каждой технологии своё, описание этих преобразований подробно изложено в книгах по нейросетевой биометрии [2.5, 2.7].

Написать программу, которая моделирует сумматор и пороговую нелинейность не сложно, однако она не будет работать, пока не будут заданы правильные значения весовых коэффициентов сумматора. Заранее во время программирования указать нужные значения весовых коэффициентов нейрона нельзя, их нужно вычислить или подобрать в процессе обучения. Структурная блок-схема итерационного алгоритма подбора весовых коэффициентов обучаемого нейрона приведена на рисунке 3.

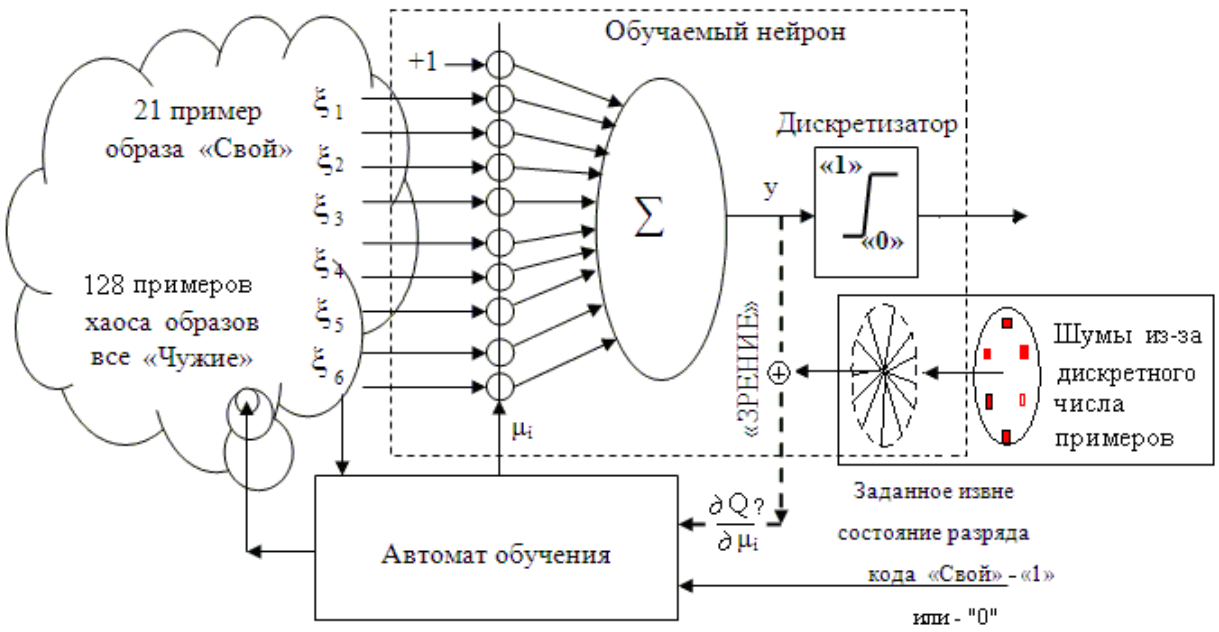



Рис. 3. Структурная блок-схема типичного итерационного алгоритма обучения нейрона

В биометрических приложениях обучение нейронов ведут на нескольких примерах образа "Свой" и нескольких десятках примеров образов "все Чужие". На данный момент в литературе по обучению искусственных нейронов описано несколько десятков алгоритмов итерационного обучения, однако все они неустойчивы. Причиной неустойчивости является малое число, используемых при обучении, примеров образа "Свой". По этой причине появляются ложные максимумы и минимумы различных критериев качества обучения. Например, алгоритмы "выталкивания" образа "Свой" на периферию распределения образов "все Чужие". Работа этого алгоритма иллюстрируется рисунком 4.

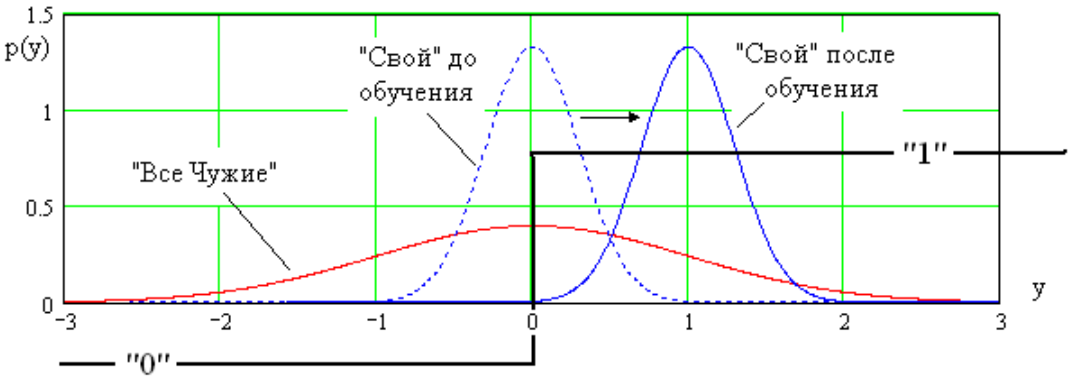



Рис. 4. "Выталкивание" распределения образов "Свой" из центра распределения образов "все Чужие" на их периферию

Из рисунка 4 видно, что у использующихся в биометрических приложениях нейронов нелинейный элемент переключается из состояния "0" в состояние "1" в центре распределения примеров образов "все Чужие". Только в этом случае удается обеспечить равновероятные состояния "0" и "1" на выходе нейрона при попытках подбора пароля или ключа.

Отклик на воздействие примерами "Свой" на необученный нейрон, как правило, находится в центре распределения "все Чужие". Процесс обучения сводится к тому, чтобы "вытолкнуть" распределение примеров "Свой" на периферию распределения образов "все Чужие". Если разряд ключа на образе "Свой" должен принимать состояние "1", то сдвигать распределение "Свой" следует в правую сторону (см. рис.4). Если разряд ключа на образе "Свой" должен принимать состояние "0", то сдвигать распределение "Свой" следует в левую сторону (см. рис.4).

Очевидно, что обученный нейрон будет узнавать "Своего" тем лучше, чем дальше на периферию удастся вытолкнуть распределение "Свой". Как следствие итерационный алгоритм обучения должен искать максимум следующего показателя качества:

$$Q = \frac{\sigma_{\text{чужие}}(y)}{\sigma_{\text{свой}}(y)} \cdot \left| E_{\text{свой}}(y) \right|, \qquad (1)$$

где y – значение отклика на выходе сумматора нейрона;

$\sigma_{\text{чужие}}(y)$ – среднеквадратическое отклонение (с.к.о.) образов "Чужие" на выходе сумматора;

$\sigma_{\text{свой}}(y)$ – с.к.о. образов "Свой";

$E_{\text{свой}}(y)$ – математическое ожидание откликов на примеры образа "Свой".

Показатель качества (1) является многомерной функцией настраиваемых весовых коэффициентов $Q(\mu_1, \mu_2, \mu_3, ...., \mu_n)$, соответственно поиск максимума показателя качества

можно вести, вычисляя частные производные $\frac{\partial Q}{\partial \mu_1}$, $\frac{\partial Q}{\partial \mu_2}$, ….., $\frac{\partial Q}{\partial \mu_n}$. Знак частных производных показывает направление, в котором следует изменять подбираемый параметр (увеличивать его или уменьшать), а значение частной производной позволяет оценить то на сколько следует изменить подбираемый весовой коэффициент.

Проблема всех итерационных алгоритмов обучения возникает из-за того, что операции численного дифференцирования неустойчивы (дифференцирование усиливает случайный шум ошибок вычислений). Сами же ошибки возникают из-за малого числа примеров "Свой" при вычислении математического ожидания $\Delta E_{свой}(y)$ и при вычислении среднеквадратического отклонения $\Delta \sigma_{свой}(y)$.

В итоге итерационные алгоритмы обучения дают достаточно высокое качество обучения, если примеров "Свой" оказывается намного больше, чем число входов у обучаемого нейрона. Если примеров "Свой" мало (меньше, чем входов у нейрона), то обучение, скорее всего, окажется неустойчивым. Неустойчивость проявляется в виде появления множества ложных минимумов и максимумов достигнутого качества (1). Примеры кривых изменения показателя качества при устойчивом и неустойчивом итерационном обучении приведены на рисунке 5.

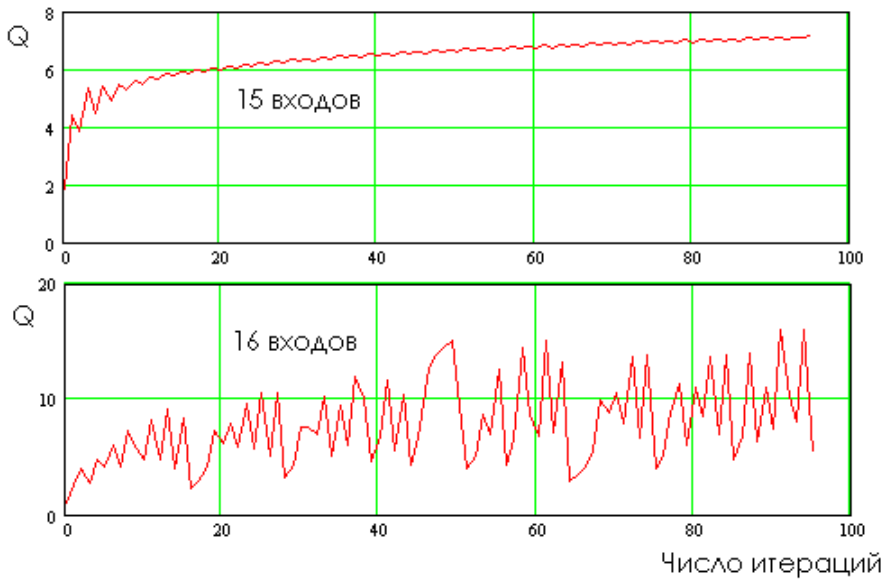



Рис. 5. Почти устойчивый режим обучения нейрона с 15 входами превращается в сильно неустойчивый режим при увеличении числа входов до 16

Если выясняется, что итерационное обучение неустойчиво, то всегда можно предпринять меры по повышению устойчивости. Для этого следует либо уменьшить число входов у нейрона, либо увеличить число примеров в обучающей выборке.

Для биометрических приложений полная автоматизация обучения нейросети принципиально важна. Появление постороннего человека (специалиста по обучению нейросети) – это угроза компрометации криптографического ключа, воспроизводить который обучается нейросеть, кроме того, возникает угроза компрометации тайного биометрического образа человека. Если же обучение нейросети ведёт автомат, то вся компрометирующая информации может быть стёрта после обучения. В свою очередь создать автомат для неустойчивого обучения крайне сложно, нет никаких гарантий, что он найдёт верное решение. В связи с этим необходимо использовать абсолютно устойчивые не итерационные алгоритмы обучения, специально созданные для нейросетевой биометрии. Один из таких алгоритмов и лёг в основу национального стандарта ГОСТ Р 52633.5.

### 1.2. Абсолютно устойчивый алгоритм автоматического обучения

Каждый входной биометрический параметр $\xi_i$ образа "Свой" имеет некоторое математическое ожидание $E(\xi_i)$ и среднеквадратическое отклонение $\sigma(\xi_i)$. Пользуясь знанием этих статистических моментов, удаётся создавать абсолютно устойчивый не итерационный алгоритм обучения "выталкиванием". Для этого необходимо отказаться от итерационного подбора весовых коэффициентов, заменив его прямым вычислением:

$$\begin{cases} \mu_i = \dfrac{\sigma_{\text{чужой}}(\xi_i)}{\sigma_{\text{свой}}(\xi_i)} E_{\text{свой}}(\xi_i) \cdot \text{sign}\left(E_{\text{свой}}(\xi_i)\right), & \text{если образ "Свой" должен дать "1";} \\ \mu_i = -\dfrac{\sigma_{\text{чужой}}(\xi_i)}{\sigma_{\text{свой}}(\xi_i)} E_{\text{свой}}(\xi_i) \cdot \text{sign}\left(E_{\text{свой}}(\xi_i)\right), & \text{если образ "Свой" должен дать "0".} \end{cases} \quad (2)$$

Такой алгоритм обучения абсолютно устойчив, так как он вообще не имеет петли обратной связи (на рис. 3 она показана пунктиром). Этот алгоритм не требует вычисления частных производных по каждому из подбираемых параметров. Влияние случайных ошибок, допущенных при вычислении статистических моментов $E(\xi_i)$ и $\sigma(\xi_i)$, входящих в выражение (2) минимизируется сумматором нейрона. Чем больше входов у нейрона, тем надежнее работает нейрон, качество его обучения (1) монотонно увеличивается при росте числа входов нейрона. Так как исчезли случайные изменения качества обучения, требования к синтезу автомата обучения оказались минимальными. Именно это обстоятельство и позволило использовать этот алгоритм как основу отечественного стандарта ГОСТ Р 52633.5. В среде моделирования "БиоНейроАвтограф" при обучении нейронов используется автомат, полностью соответствующий требованиям Российского стандарта ГОСТ Р 52633.5.

Принятие ТК 362 (Защита информации) стандарта ГОСТ Р 52633.5 кардинально меняет ситуацию не только в биометрии, но и в других приложениях искусственного интеллекта. До принятия этого отечественного стандарта было "хорошим" правилом "выбрасывать" плохие данные и использовать меленькие нейронные сети. Однако маленькие нейронные сети ни на что приличное не способны, они всегда работают хуже, чем человек. Большие искусственные нейронные сети работают лучше человека, но обучать их до появления стандарта ГОСТ Р 52633.5 мы не умели. Так попытка обучить двухслойную нейронную сеть с 32 входами и 16 выходами методом обратного распространения ошибок с помощью какого-либо коммерческого средства математического моделирования приводит к тому, что память вычислительной машины кончается. Попытка организовать подкачку памяти с винчестера приводит к фатальному замедлению вычислений, процесс обучения полносвязной сети, имеющей всего 32*16+16*16=768 настраиваемых итерационно весовых коэффициентов, длится более 8 часов. Все это является следствием неустойчивости операций дифференцирования, используемых при обучении методом обратного распространения ошибок. При попытках обучить большую нейронную сеть на "плохих" биометрических данных все итерационные методы обучения 99.9999% вычислительного времени тратят на минимизацию многомерной поверхности ошибок собственных вычислений и только 0.000001 времени идет на полезную составляющую вычислений.

Совершенно иная ситуация возникает, когда используются абсолютно устойчивые не итерационные алгоритмы обучения родственные алгоритму ГОСТ Р 52633.5. Эти алгоритмы способны работать с любыми сколь угодно "плохими" биометрическими данными. По этой причине вместо 32 наиболее "хороших" биометрических данных можно использовать 416 младших коэффициентов двухмерного преобразования Фурье кривых X(t), Y(t) без их сортировки на "хорошие" и "плохие", как это делается в среде моделирования "БиоНейроАвтограф". "Плохих" данных всегда намного больше, чем "хороших". В нашем случае плохих данных будет 416-32=384 или в 384/32=12 раз больше

"хороших". При этом суммарный информационный вклад большого числа "плохих" данных больше, чем "хороших" в принимаемых большой нейронной сетью решениях.

В среде моделирования "БиоНейроАвтограф" используется однослойная нейронная сеть с 416 входами, 256 нейронами, каждый нейрон имеет по 24 входа. Итого при обучении вычисляются 256*24=6144 параметра за время порядка 0.1 секунды (это легко проверить). Получается, что выигрыш по времени от использования алгоритма отечественного стандарта в сравнении с популярным на данный момент методом обратного распространения ошибок составляет более чем 3 000 000 раз. Кроме того, метод обратного распространения ошибок не способен обучать нейронные сети с 3, 4, 5,… слоями нейронов, а подобных ограничений у абсолютно устойчивых не итерационных алгоритмов нет. Они могут обучать сети искусственных нейронов с любым числом слоёв нейронов, хотя ГОСТ Р 52633.5 рекомендует применять в биометрических приложениях только однослойные и двухслойные нейронные сети.

### 1.3. Быстрые алгоритмы тестирования вероятности ошибок пропуска "Чужого"

Переход к использованию больших нейронных сетей, принимающих решения высокого качества, позволяет в миллионы раз снизить вероятность ошибочного пропуска "Чужого". Это очень хорошо, однако в доверенных приложениях нужно подтверждать достигнутый при очередном обучении показатель качества, что становится проблемой. Предположим, что вероятность ошибок составляет $10^{-12}$, для того чтобы подтвердить столь малую вероятность обычными методами нужно использовать как минимум $10^{13}$ биометрических образа. Если речь идет об отпечатках пальцев, то для получения базы с $10^{13}$ биометрическими образами придётся снять отпечатки у всех жителей Земли в 100 поколениях. Время активной жизни одного поколения 30 лет, таки образом придётся собирать данные 3 000 лет. Пытаться собирать большие базы тестовых биометрических образов – это абсолютно тупиковый путь.

В связи с этой проблемой ГОСТ Р 52633.3 требует отказаться от примитивных процедур использования больших баз данных и поиска по ним редко встречающихся коллизий "Свой" – "Чужой". Национальный стандарт рекомендует перейти от статистического исследования кодов "Чужой" в обычном их представлении к статистическому исследованию распределений расстояний Хемминга между кодами "Чужой" и кодом "Свой":

$$h = \sum_{i=1}^{256} c_i \oplus x_i , \qquad (3)$$

где $\oplus$ – операция сложения по модулю два; $c_i$ – i-тый разряд кода "Свой"; $x_i$ – i-тый разряд кода "Чужой".

Выигрыш от топологического перехода в пространство расстояний Хемминга состоит в возможности отказа от тактики ожидания появления редких событий и переход к тактике предсказания вероятности появления редких событий. Возможность этого перехода опирается на то, что распределение расстояний Хемминга сравниваемых кодов длиной 256 бит является нормальным. Эта ситуация отражена на рисунке 6.

Для того чтобы предсказать вероятность появления редкого события $h_i=0$ в рамках гипотезы о нормальном законе распределения значений, достаточно вычислить математическое ожидание расстояний Хемминга и его среднеквадратическое отклонение по выборке, например, из 200 кодов:

$$\begin{cases} E(h) = \dfrac{1}{200}\sum_{i=1}^{200} h_i \\ \sigma(h) = \sqrt{\dfrac{1}{200}\sum_{i=1}^{200} (E(h) - h_i)^2} \end{cases} \qquad (4)$$

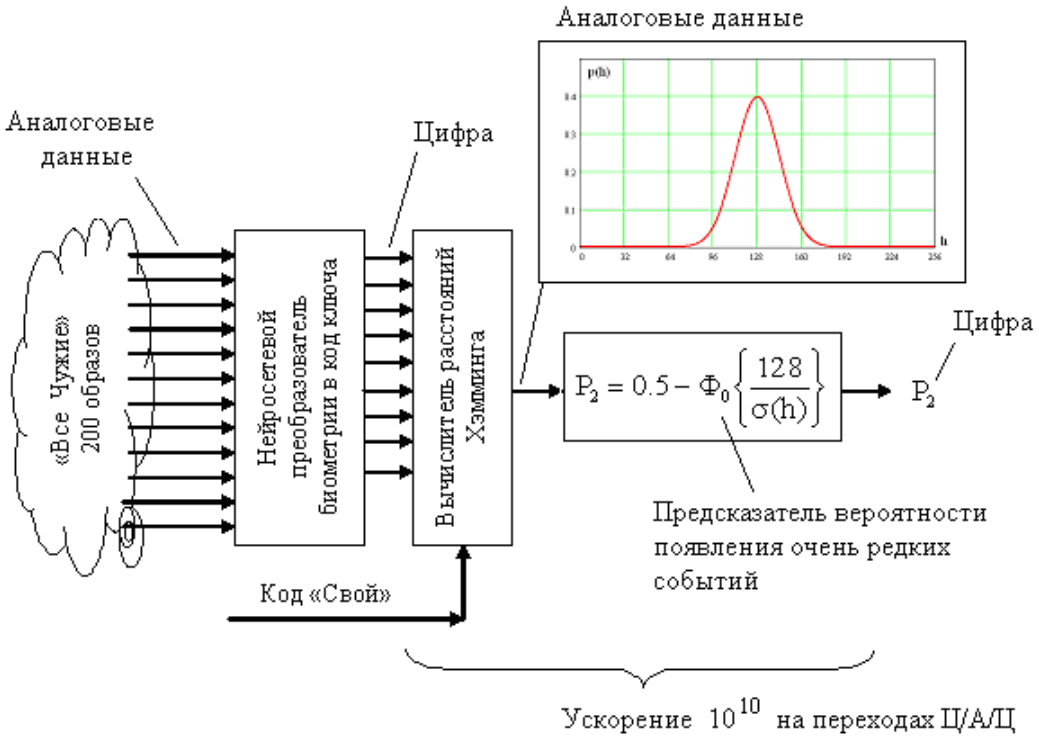



Рис. 6. Прогнозирование вероятности ошибок второго рода
на 200 образах "Чужой" по ГОСТ Р 52633.3-2011

Далее необходимо вычислить вероятность появления коллизии кодов "Свой" и "Чужой":

$$P_2 = \frac{1}{\sigma(h)\sqrt{2\pi}} \int_{-\infty}^{1} \exp\left\{\frac{-(E(h)-u)^2}{2\sigma^2(h)}\right\} du \qquad (5)$$

Из-за того, что мы отказываемся от ожидания редких событий и начинаем их предсказывать, возникают огромные ускорения времени вычислений. В частности отказ от просмотра базы из $10^{13}$ образов и использование базы всего из 200 образов приводит к ускорению вычислений в $10^{10}$ раз.

### 1.4. Быстрые алгоритмы тестирования вероятности ошибок отказа "Своему"

При тестировании больших нейронных сетей возникает ещё одна проблема, связанная с оценкой вероятности ошибок первого рода на малых тестовых выборках. Предположим, что производитель заявил очень высокие вероятностные характеристики своего средства аутентификации. Чтобы подтвердить значение вероятности ошибок отказа "Своему" на уровне $10^{-2}$ потребуется примерно 200 тестовых образов "Свой", не участвовавших в обучении. Что бы воспроизвести 200 образов потребуется время пользователя, а пользователь – это потребитель. Потребитель всегда прав, заставлять его делать лишнюю работу нежелательно. В связи с этим необходимо отказаться от обычных методик тестирования, перейти к малым обучающим выборкам из 20 примеров и за счёт предсказания давать точный прогноз вероятности появления ошибок.

Исследования, проведенные в ОАО "ПНИЭИ" показали, что распределение расстояний Хемминга сильно коррелированных образов "Свой" хорошо описывается $\chi^2$ распределением с малым числом степеней свободы. Из теории известно, что математическое ожидание величины, описываемой $\chi^2$ распределением, имеет совпадающее с математическим ожиданием число степеней свободы:

$$m = E(h) = \frac{1}{20}\sum_{i}^{20} h_i \qquad (6)$$

То есть оценив математическое ожидание расстояний Хемминга 20 тестовых примеров, мы получаем оценку числа степеней свободы распределения $\chi^2$. Далее в рамках гипотезы $\chi^2$ распределения мы можем найти оценку вероятности появления ошибок первого рода:

$$P_1 = \int_0^1 p(\chi^2(m,h)) \cdot dh \qquad (7)$$

Интеграл следует вычислять пользуясь калькулятором ошибок первого рода, поставляемым совместно со средой моделирования "БиоНейроАвтограф" (см. раздел 5 данного учебного пособия).

### 1.5. Вычисление высокоразмерной энтропии по Шеннону и Хеммингу

Вычисление энтропии выходных кодов является одним из самых эффективных математических инструментов исследования последовательностей кодов. По Шеннону для некоторой конечной системы кодов (например, кодов букв языка) может быть вычислена энтропия этой системы через вероятности появления того или иного кода в анализируемой последовательности. Энтропию одиночных кодов обычно оценивают через вероятности их появления:

$$H(x) = -\sum_{i=1}^{S} P(x_i) \cdot \log_2(P(x_i)), \qquad (8)$$

где $x$ – кодировка одиночной буквы (знака) сообщения;

$i$ – порядковый номер одиночной буквы (знака) сообщения в алфавите;

$S$ – общее число букв (знаков) в языке (алфавите) сообщения,

$P(x_i)$ – вероятность появление кода $x_i$.

Необходимо отметить, что выражение (8) описывает энтропию появления одиночных символов (например, букв некоторого языка). Такая оценка энтропии корректна только в первом приближении. Для более точного описания энтропии системы (например, естественного языка) необходимо учитывать энтропию появления пар букв:

$$H(x_1, x_2) = -\sum_{1i=1}^{S} \sum_{2i=1}^{S} P(x_{1i}, x_{2i}) \cdot \log_2(P(x_{1i}, x_{2i})), \qquad (9)$$

где $x_1$ – кодировка первой буквы (знака) в паре знаков сообщения;

$x_2$ – кодировка второй буквы (знака) в паре знаков сообщения.

Очевидно, что по аналогии с выражениями (8) и (9) могут быть построены выражения для энтропии трёх букв, четырёх букв и так далее. В итоге для вычисления энтропии группы из "n" символов мы получим следующее выражение:

$$H(x_1, x_2, ..., x_n) = -\sum_{1i=1}^{S} \sum_{2i=1}^{S} ..... \sum_{ni=1}^{S} P(x_{1i}, x_{2i}, ..., x_{ni}) \cdot \log_2(P(x_{1i}, x_{2i}, ..., x_{ni})) \qquad (10)$$

Идеология вычисления многомерной энтропии, хорошо отработанная для кодировок текста, может быть применена и для оценки энтропии выходных кодов. Применительно к нейросетевому преобразователю среды моделирования "БиоНейроАвтограф" преобразования (8), (9), (10) можно записать следующим образом:

$$H(256) = -\sum_{i=1}^{2^{256}} P(256_i) \cdot \log_2(P(256_i)), \quad (11)$$

где $P(256_i)$ – вероятность появления i-того кода длиной 256 бит.

Вычислять энтропию по формуле (11) затруднительно, так как нужно иметь очень большую выборку исходных данных. Прямое вычисление энтропии через выражение (11) технически невозможно, в связи с этим будем ориентироваться на выборку всего из 200 кодов "Чужой":

$$H(256) = -\sum_{i=1}^{200} \tilde{P}(256_i) \cdot \log_2(\tilde{P}(256_i)), \quad (12)$$

где $\tilde{P}(256_i)$ – вероятность появления i-того кода длиной 256 бит, вычисленная в пространстве распределения расстояний Хемминга между i-тым кодом и другими 199 кодами исследуемой выборки из 200 примеров.

Из теории известно, что значение многомерной энтропии сильно зависит от коррелированности разрядов исследуемых кодов H(256,E(|r|)). Если корреляционные связи между разрядами кодов отсутствуют, то энтропия максимальна:

$$H(256,E(|r|)) = 256 \text{ бит}, E(|r|) = 0 \quad (13)$$

Если корреляция предельно велика, то энтропия минимальна:

$$H(256,E(|r|)) = 1 \text{ бит}, E(|r|) = 1 \quad (14)$$

Можно построить функцию для 256 мерной энтропии связи её значения с математическим ожиданием модулей коэффициентов парной корреляции. Эта работа была выполнена, и соответствующая номограмма приведена в [2.5]. Подобные функции (номограммы связи) сложны для практического применения, это является следствием попытки увязать между собой совершенно разные по своей сути характеристики многомерную энтропию и обычную двухмерную корреляцию. Снизить сложность связи удаётся введением промежуточной переменной (многомерной корреляции R(256)) с последующим понижением размерности корреляции до двухмерной. Промежуточная переменная вводится следующим образом:

$$R(256) = (1 - \frac{H(256, E(|r|)}{H(256, E(|r| = 0)}) = (1 - \frac{H(256, E(|r|))}{256}) = (1 - \frac{H(256, \tilde{r})}{256} \quad (15)$$

В свою очередь функции $R(512, \tilde{r})$, $R(256, \tilde{r})$, $R(128, \tilde{r})$, …., $R(2, \tilde{r})$, $R(1, \tilde{r})$ оказываются достаточно просты и уже могут быть применены в инженерных расчётах. Номограмма с этими функциями приведена на рисунке 7.

Из рисунка 7 видно, что функция дробной размерности R(15,471) точно совпадает с прямой:

$$R(n, \tilde{r}) = \tilde{r}, \; n = 15,471 \quad (16)$$

Кроме того, значительные участки кривых $R(n, \tilde{r})$ очень хорошо приближаются отрезками прямых, а сшивка соединений прямых хорошо осуществляется фрагментами окружностей.

Параметры аппроксимирующих прямых, а так же точки сшивки и радиусы сшивающих приближение окружностей приведены в таблице 1.

Дробная размерность $n \approx 15.5$ играет роль границы между высокоразмерными системами и низкоразмерными системами (нейросетевыми преобразователями). Энтропия для высокоразмерных преобразователей (больших искусственных нейронных сетей) и энтропия для низкоразмерных преобразователей (маленьких искусственных нейронных сетей) ведёт себя совершенно по-разному. Функции, описывающие высокоразмерные и

низкоразмерные корреляции, по-разному выгнуты относительно границы n≈15.5. Тот результат, который дают высокоразмерные преобразования для n>15.5 никогда не может быть достигнут низкоразмерными нейросетевыми преобразованиями.

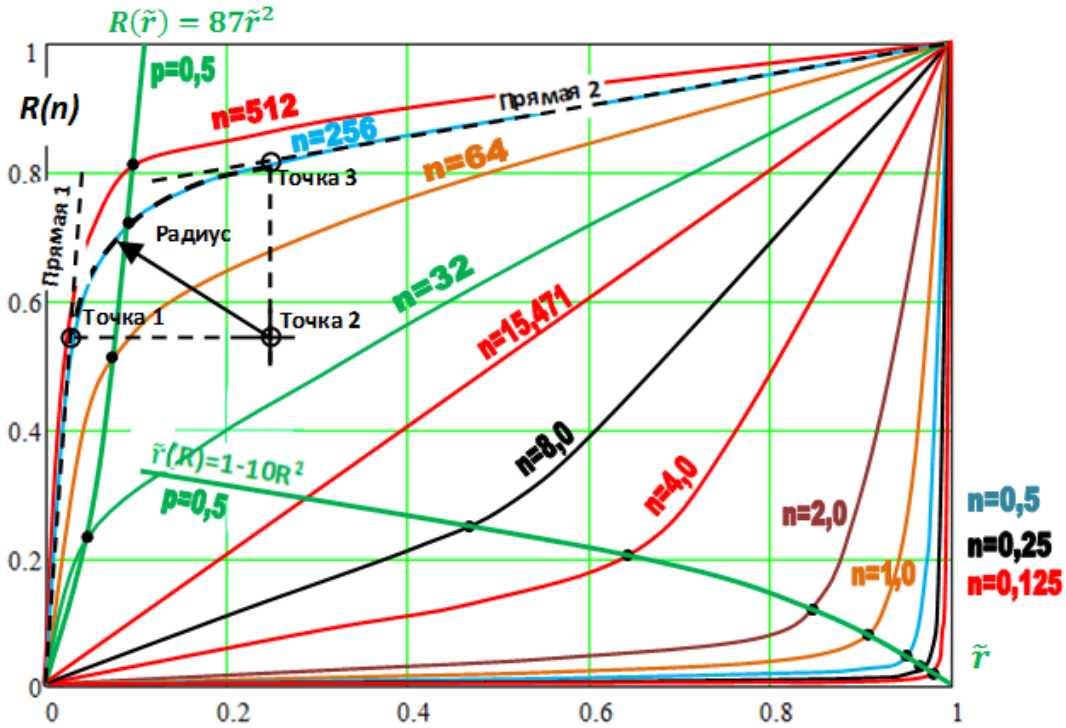



Рис. 7. Номограмма связи значений многомерной корреляции R(n) с обобщенным значением корреляции, равным математическому ожиданию модулей парных значений коэффициентов корреляции.

Таблица №1

| | | Линия 1 | Линия 2 | Точка 1 | Точка 2 | Точка 3 | Радиус |
|---|---|---|---|---|---|---|---|
| Размерность | n=0.125 | $R(\tilde{r}) = 0.03\tilde{r}$ | $R(\tilde{r}) = 74\tilde{r} - 73$ | (0.96;0.08) | (0.95;0.1) | (0.98:0.06) | 0.02 |
| | n=0.25 | $R(\tilde{r}) = 0.04\tilde{r}$ | $R(\tilde{r}) = 43\tilde{r} - 42$ | (0.94;0.1) | (0.93:0.12) | (0.97;0.08) | 0.03 |
| | n=0.5 | $R(\tilde{r}) = 0.05\tilde{r}$ | $R(\tilde{r}) = 28\tilde{r} - 27$ | (0.92;0.12) | (0.91;0.14) | (0.96;0.1) | 0.04 |
| | n=1 | $R(\tilde{r}) = 0.06\tilde{r}$ | $R(\tilde{r}) = 12\tilde{r} - 11$ | (0.86;0.05) | (0.84;0.12) | (0.93;0.17) | 0.06 |
| | n=2 | $R(\tilde{r}) = 0.07\tilde{r}$ | $R(\tilde{r}) = 8\tilde{r} - 7$ | (0.8;0.08) | (0.72;0.24) | (0.88;0.2) | 0.1 |
| | n=4 | $R(\tilde{r}) = 0.3\tilde{r}$ | $R(\tilde{r}) = 2.5\tilde{r} - 1.5$ | (0.55;0.17) | (0.48;0.42) | (0.73;0.33) | 0.14 |
| | n=8 | $R(\tilde{r}) = 0.5\tilde{r}$ | $R(\tilde{r}) = 1.5\tilde{r} - 0.5$ | (0.4;0.2) | (0.35;0.45) | (0.6;0.4) | 0.4 |
| | n=16 | $R(\tilde{r}) = 1.1\tilde{r}$ | $R(\tilde{r}) = 0.98\tilde{r} + 0.02$ | (0.08;0.07) | (0.5;-0.4) | (1.3;1.4) | 0.56 |
| | n=32 | $R(\tilde{r}) = 9\tilde{r}$ | $R(\tilde{r}) = 0.75\tilde{r} + 0.25$ | (0.01;0.18) | (0.4;-0.2) | (0.1;0.3) | 0.38 |
| | n=64 | $R(\tilde{r}) = 12\tilde{r}$ | $R(\tilde{r}) = 0.4\tilde{r} + 0.6$ | (0.02;0.4) | (0.3;0.2) | (0.15;0.62) | 0.32 |
| | n=128 | $R(\tilde{r}) = 15\tilde{r}$ | $R(\tilde{r}) = 0.35\tilde{r} + 0.65$ | (0.03;0.47) | (0.28;0.44) | (0.15;0.74) | 0.3 |
| | n=256 | $R(\tilde{r}) = 18\tilde{r}$ | $R(\tilde{r}) = 0.25\tilde{r} + 0.75$ | (0.04;0.55) | (0.26;0.58) | (0.26;0.81) | 0.27 |
| | n=512 | $R(\tilde{r}) = 21\tilde{r}$ | $R(\tilde{r}) = 0.2\tilde{r} + 0.8$ | (0.05;0.6) | (0.24;0.6) | (0.24;0.84) | 0.2 |

Для низкоразмерных преобразований каждый шаг по повышению размерности решаемой задачи приводит к увеличению проблем, которые на математическом сленге образно обозначаются как "проклятие размерности". Граница n≈15.5 это некоторый барьер, пробив который мы попадаем в совершенно другую область "благодати высоких и сверхвысоких размерностей". Наше естественное нейросетевое подсознание как раз и работает в области "благодати высоких и сверхвысоких размерностей", ГОСТ Р 52633.5 впервые уровнял возможности естественного подсознания человека и искусственного нейросетевого подсознания биометрических приложений http://пниэи.рф/activity/science/bio_neuro.pdf.

# 2. Возможности среды моделирования "БиоНейроАвтограф"

## 2.1. Запуск среды моделирования "БиоНейроАвтограф"

Зайдите на страницу http://пниэи.рф/activity/science/noc.htm, скачайте архив bioneuroautograph.zip. Распакуйте архив и запустите находящийся в папке файл БиоНейроАвтограф.exe. При этом появится основная экранная форма с фотографией административного здания ОАО "ПНИЭИ" г. Пенза, улица Советская, 9.

## 2.2. Как задать пароль доступа или криптографический ключ

Среда моделирования "БиоНейроАвтограф" предназначена для нейросетевого связывания рукописного пароля с обычным паролём доступа (набираемым на клавиатуре) или криптографическим ключом. Пароль доступа может быть изменён по усмотрению студента. Для того чтобы задать или изменить пароль необходимо выбрать пункт меню "Режим", подпункт "Задать пароль" в левом верхнем углу основного диалогового окна (рис. 8). Или одновременно нажать комбинацию клавиш "Ctrl+P".

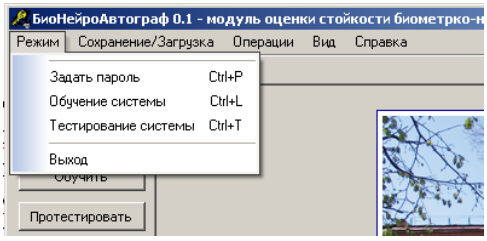



Рис. 8. Выбор пункта меню "Задать пароль".

При этом появится окно создания пользовательского пароля с двумя полями ввода (рис. 9). В верхнем поле введите имя пользователя (свой логин), в нижнем введите свой пароль, состоящий, например, из 32-х символов "a" в латинской кодировке.

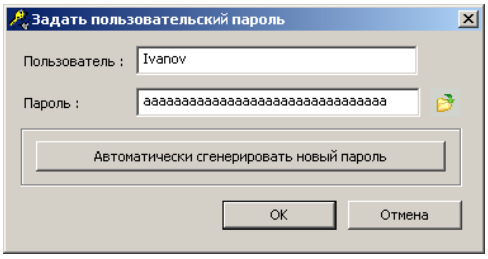



Рис. 9. Диалоговое окно создания пароля

Для создания длинного случайного пароля нажмите кнопку "Автоматически сгенерировать новый пароль". Сгенерированный 32-х символьный пароль при обучении преобразуется в обучающий ключ длиной 256 бит (32 случайных символа в 8 битной кодировке). Сохранение введённого имени пользователя и пароля происходит после нажатия кнопки "ОК". В случае успешного сохранения данных можно приступать к обучению нейронной сети.

## 2.3. Как обучить нейронную сеть

Обучение нейронной сети осуществляется в режиме обучения (рис. 10), который вызывается с помощь нажатия кнопки "Обучить" основного меню, либо выбором пункта меню "Режим", подпункт "Обучение системы", либо одновременным нажатием комбинации клавиш "Ctrl+L".

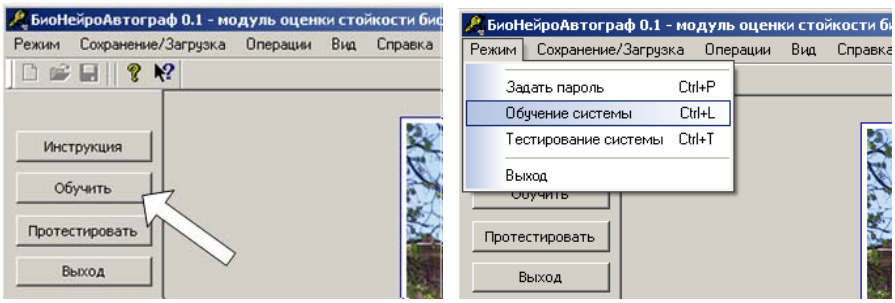


Рис. 10. Вызов режима обучения

Для того чтобы обучить нейронную сеть необходимо ввести несколько обучающих примеров той или иной рукописной буквы или рукописного слова. Если пользоваться манипулятором "мышь", то лучше вводить примеры отдельных букв, либо короткие слова, т.к. писать с помощью "мышки" достаточно сложно. Если имеется графический планшет, то для обучения необходимо вводить рукописное слово, состоящее из трех и более букв. При выборе обучающего символа или слова необходимо знать, что чем длиннее вводимое слово и чем выше стабильность его написания, тем выше стойкость обученной сети к атакам подбора. Так как с помощью манипулятора "мышь" вводить длинные стабильные слова невозможно, то качество обучения будет низким, а вероятности появления ошибок высокими.

После входа в режим обучения введите с помощью манипулятора "мышь" или графического планшета несколько примеров выбранного для обучения рукописного слова или рукописной буквы.

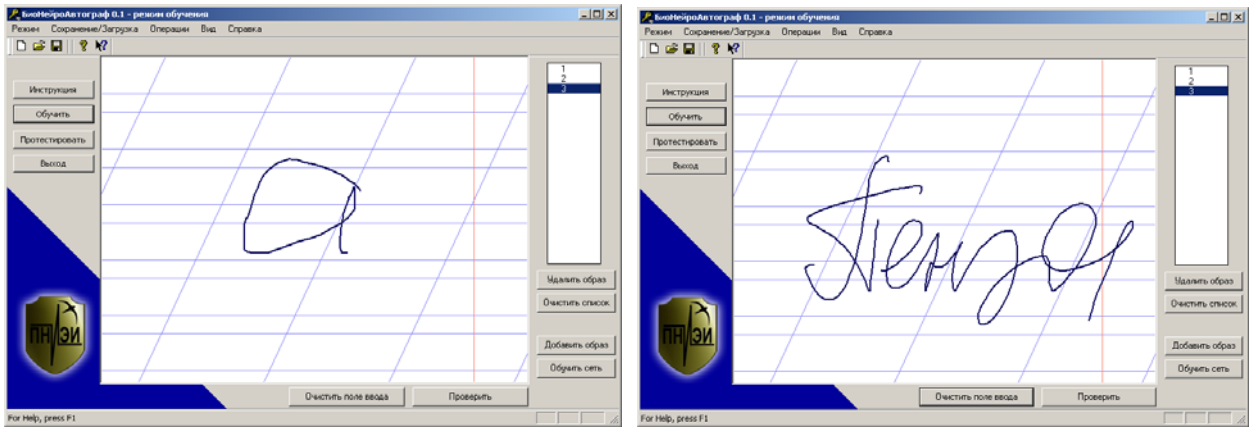


Рис. 11. Диалоговое окно обучения нейронной сети

После каждого ввода примера обучающего слова, необходимо добавить введённый пример в список обучающих примеров (список в правом верхнем углу диалогового окна обучения). Добавление примера осуществляется нажатием кнопки "Добавить образ" в правом нижнем углу диалогового окна.

Все ранее введенные примеры могут быть просмотрены щелчком манипулятора "мышь" по соответствующему номеру примера в списке обучающих примеров. Если добавленный в список пример неудачен (например, дрогнула рука), то его можно удалить. Для этого необходимо выбрать неудачный пример в списке обучающих примеров и нажать кнопку "Удалить образ". Чтобы удалить все обучающие примеры из списка нажмите кнопку "Очистить список".

Удаление текущего введённого рукописного образа и очистка поля ввода осуществляется с помощью кнопки "Очистить поле ввода".

После добавления в список обучающих примеров трёх или более примеров рукописного образа, запустите процесс обучения нейронной сети, нажав кнопку "Обучить сеть". Обучение сети из 256 нейронов длится менее одной секунды. По окончанию

обучения появляется окно с результатами обучения (рис. 12), содержащее информацию о предполагаемой стабильности введенных биометрических примеров, вероятности узнавания образа "Свой" и ожидаемой стойкости системы к атакам подбора обучающего рукописного слова-пароля, т.е. вероятность пропуска образа "Чужой".

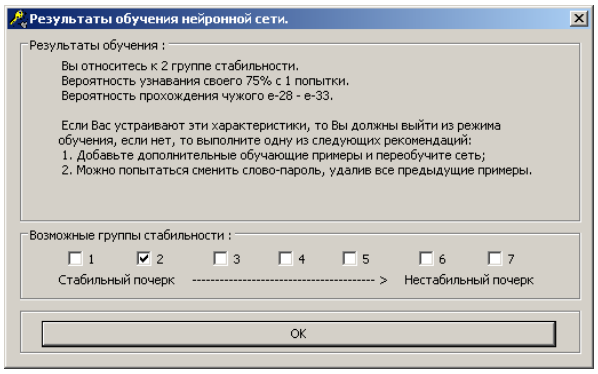



Рис. 12. Окно с результатами обучения

Можно попытаться изменить качество обучения, увеличивая или уменьшая число примеров обучения. Более точную оценку качества обучения можно дать только после тестирование искусственной нейронной сети. Доверие к результатам обучения, отображаемым в окне с результатами обучения, низкое, так как эти данные рассчитывались по обучающей выборке.

### 2.4. Как проверить обученную нейронную сеть

Для того чтобы получить достоверную оценку качества обучения необходимо в поле ввода рукописных образов ввести пример рукописного образа "Свой" и нажать кнопку "Проверить". При этом вычисляются параметры введенного рукописного образа, они подаются на входы искусственной нейронной сети, вычисляется выходной код и выводится окно с результатами сравнения полученного выходного кода с обучающим кодом (рис. 13).

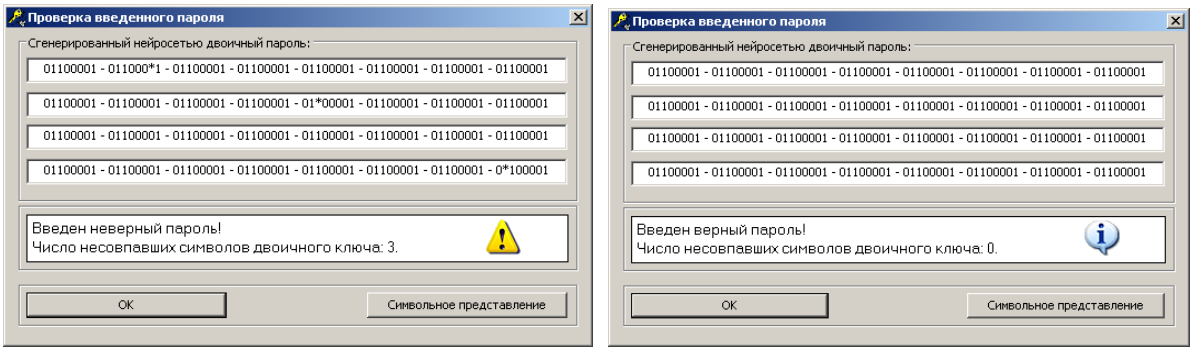



Рис. 13. Окно вывода полученного кода на примерах образа "Свой"

Сеть хорошо узнаёт образ "Свой", если мера Хемминга на тестовых примерах равно нулю (все разряды полученного кода совпадают с заданным при обучении кодом "Свой"). Если несколько бит кодов не совпадают, то обучение нужно продолжить, добавив в обучающую выборку дополнительные примеры рукописного образа "Свой". Хорошо обученная нейронная сеть должна с высокой вероятностью узнавать образ "Свой".

Для проверки способности нейронной сети отказывать в доступе образам "Чужой" необходимо воспроизвести случайное рукописное слово (букву). При этом появляется случайный код, совпадающий с кодом "Свой" в случайных разрядах. В окне вывода

полученного кода совпавшие разряды отображаются верными состояниями "0" и "1", а несовпавшие разряды отображаются символом "*" (рис. 14).

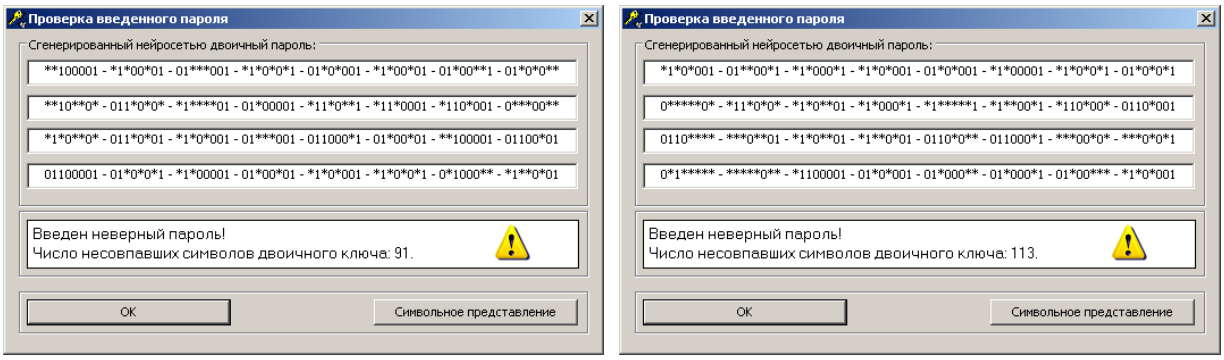



Рис. 14. Окно вывода полученного кода на примерах образа "Чужой"

Даже в том случае, когда воспроизводится один и тот же случайный рукописный образ "Чужой" выходные коды нейросети должны быть случайными (отличающиеся состояния должны располагаться в разных разрядах кодов).

Стойкость обученной нейронной сети тем выше, чем ближе число отличающихся разрядов кода к величине 128. Так как для действительно случайных состояниях выходного кода "Чужой" с наибольшей вероятностью угадывает примерно половину из 256 разрядов кода.

### 2.5. Как сохранить и загрузить биометрические образы

Для того чтобы надёжно тестировать качество работы обученного преобразователя биометрия-код нужно создавать специальные базы тестовых образов "Свой" и "Чужой" по требованиям ГОСТ Р 52633.1-2009. Средство моделирования большой нейронной сети "БиоНейроАвтограф" имеет встроенные средства, позволяющие собирать базы биометрических образов.

Сохранение обучающей выборки примеров "Свой" осуществляется путём выбора пункта меню "Сохранение/Загрузка", подпункта "Сохранить образы на диск", либо одновременным нажатием комбинации клавиш "Ctrl+S" (рис. 15).

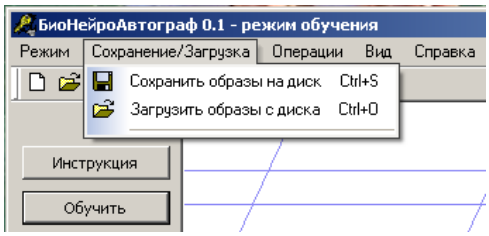



Рис. 15. Пункт меню сохранения и загрузки образов

Далее в открывшемся диалоговом окне укажите каталог, в котором будет сохранён файл, и задайте имя файла (по-умолчанию задано имя "MyImages.dat"). Рекомендуется примеры, на которых производилось обучение, сохранять с именем "Обучение__.dat", а примеры для тестирования обозначать именами "Тестирование_СВОЙ_.dat" или "Тестирование_ЧУЖИЕ_.dat".

После успешного сохранения можно удалить все обучающие примеры.

Сохранённые ранее примеры рукописных образов всегда можно загрузить и повторно обучить нейронную сеть. Загрузка рукописных образов осуществляется путём выбора пункта меню "Сохранение/Загрузка", подпункта "Загрузить образы с диска", либо одновременным нажатием комбинации клавиш "Ctrl+O" (рис. 15).

В появившемся диалоговом окне выберите требуемый файл с образами и нажмите кнопку "Открыть", загруженные примеры автоматически добавляются в список обучающих примеров.

Режим сохранения и загрузки рукописных образов крайне важен для формирования больших баз биометрических образов, например, при выполнении лабораторной работы №6. У людей существует порог "комфортности" требований к ним со стороны биометрических автоматов. Мы легко пишем подряд десяток рукописных слов, однако требование воспроизвести подряд 20 одинаковых слов уже воспринимается людьми как некоторое обременение. Требование воспроизвести своею рукой 200 одинаковых слов людьми воспринимается как существенное обременение (нужно написать страницу рукописного текста). В связи с этим сохранение образов и обмен базами "все Чужие" – это мера, позволяющая существенно снизить трудоемкость лабораторных работ.

Следует иметь в виду, что режим "Сохранение/Загрузка" есть только у учебных средств моделирования искусственных нейронных сетей. Реальные средства биометрико-нейросетевой аутентификации должны уничтожать данные обучения и тестирования по требованиям ГОСТ Р 52633.0-2006.

## 2.6. Специальные режимы работы

### 2.6.1. Режим, воспроизводящий биометрическую аутентификацию

Среда моделирования "БиоНейроАвтограф" ориентирована на студентов занимающихся изучением применения нейросетевого искусственного интеллекта к приложениям защиты информации. В связи с этим в этой среде реализован режим, имитирующий меню программного средства биометрической аутентификации. Попасть в этот режим можно через основное меню, нажав кнопку "Протестировать", либо выбрав пункт меню "Режим", подпункт "Тестирование системы", либо одновременным нажатием комбинации клавиш "Ctrl+T". Главное диалоговое окно тестирования работы нейронной сети в режиме аутентификации пользователей представлено на рисунке 16.

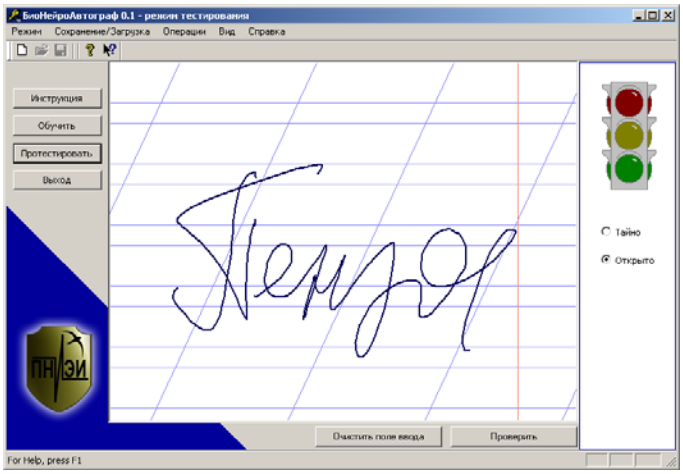



Рис. 16. Диалоговое окно режима тестирования

В правом верхнем углу диалогового окна расположен светофор с тремя состояниями: красный, жёлтый и зелёный. В случае положительного результата аутентификации загорается зелёный свет светофора. Если введённый биометрический образ близок к эталонному образу "Свой", загорается жёлтый свет светофора. Если введённый биометрический образ далек от эталонного образа "Свой", загорается красный свет. Светофор помогает пользователю "Свой" ориентироваться в текущем состоянии протокола биометрико-криптографической аутентификации. Индикатор состояния,

выполненный в форме светофора безопасен, так как выполнен в соответствии с требованиями ГОСТ Р 52633.6.

Особенно важен светофор в режиме "Тайно", когда пользователь аутентифицируется по рукописному слову-паролю, которое не отображается на экране видеомонитора. Режим "Тайно" применяется пользователем в ситуации присутствия рядом с ним посторонних лиц. Режим "Открыто" применяется пользователем, когда он один, и никто не может подсмотреть его тайный рукописный пароль.

Основное отличие режима аутентификации от режимов обучения и тестирования состоит в том, что в этом режиме ключ "Свой" неизвестен, следовательно невозможно вычислить количество отличающихся бит ключа и показать их позиции. Так как в режиме аутентификации сравниваются не ключи/пароли, а хеш-код полученного ключа с хеш-кодом эталонного, то отображается только сигнал светофора и выводится сообщение с результатами проверки введённого пароля.

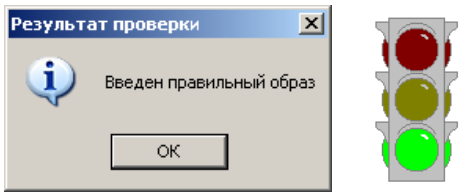



Рис. 17. Аутентификация пройдена

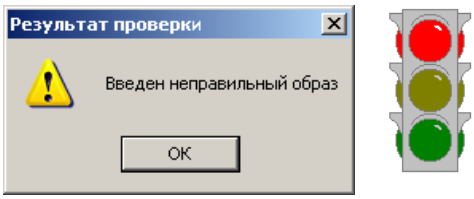



Рис. 18. Аутентификация не пройдена

Жёлтый сигнал светофора выдаётся вместе с сообщением "Введен неправильный образ". Подробнее об этом состоянии можно узнать, выполнив лабораторную работу № 10.

### 2.6.2. Режим автоматического тестирования на базе тестовых образов

В случае, когда тестовая база создана заранее, можно воспользоваться специальным режимом тестирования на образах из базы. Для этого необходимо выбрать пункт меню "Операции", подпункт "Тестировать на тестовых образах" (рис. 19).

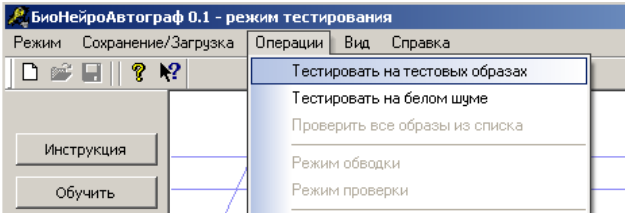



Рис. 19. Запуск тестирования на реальных образах

В результате появляется диалоговое окно выбора каталога, в котором хранятся файлы с тестовыми рукописными образами. После выбора нужного файла и нажатия кнопки "Открыть" запускается процесс тестирования обученной нейронной сети на выбранных образах. После завершения процесса тестирования выводится окно с результатами проверки (рис. 20).

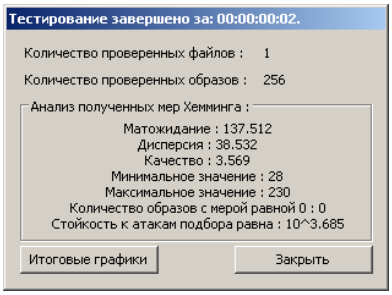



Рис. 20. Окно с результатами тестирования

Окно результатов содержит информацию о количестве использовавшихся во время тестирования примеров реальных рукописных образов, математическое ожидание, среднеквадратическое отклонение, качество, минимальное и максимальное значение полученных мер Хемминга. Также отображается количество "взломов" системы (количество образов с нулевой мерой) и вычисленная на тестовой базе стойкость к атакам подбора. Все вычисляемые во время тестирования меры Хемминга записываются в файл Data/<Имя_пользователя>/mera.txt. Каталог Data находится рядом с запускаемым файлом БиоНейроАвтограф.exe. После каждого тестирования происходит перезаписывание данных в файле mera.txt.

ПРИМЕЧАНИЕ. В каталоге Data также хранятся весовые коэффициенты обученной нейронной сети в файле weights.txt; а в файле coefs.txt хранятся коэффициенты двухмерного преобразования Фурье последнего поданного на нейронную сеть примера биометрического образа.

### 2.6.3. Режим автоматического тестирования на "белом шуме"

Если нет корректно собранной базы биометрических образов, то тестирование может быть выполнено на данных, получаемых от генератора случайного шума, т.е. тестирование на искусственно синтезированных образах. Для запуска тестирования на белом шуме необходимо выбрать пункт меню "Операции", подпункт "Тестировать на белом шуме" (рис. 21).

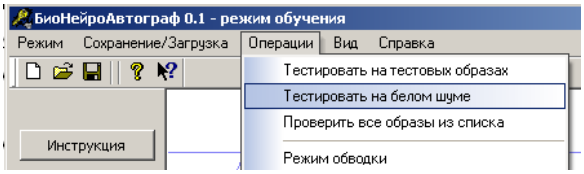



Рис. 21. Запуск тестирования на синтезированных образах

Тест запускается автоматически. Тестирование обученной нейронной сети осуществляется на 1 000 сгенерированных примерах рукописных образов. После завершения процесса тестирования выводится окно с результатами проверки (рис. 22).

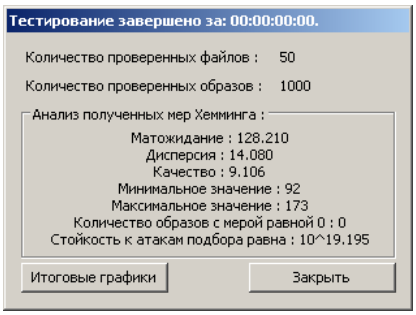



Рис. 22. Окно с результатами тестирования

Окно результатов содержит информацию о количестве использовавшихся во время тестирования примеров реальных рукописных образов, математическое ожидание,

среднеквадратическое отклонение, качество, минимальное и максимальное значение полученных мер Хемминга. Также отображается количество "взломов" системы (количество образов с нулевой мерой) и вычисленная на тестовой базе стойкость к атакам подбора. Все вычисляемые во время тестирования меры Хемминга записываются в файл Data/<Имя_пользователя>/mera.txt. Каталог Data находится рядом с запускаемым файлом БиоНейроАвтограф.exe. После каждого тестирования происходит перезаписывание данных в файле mera.txt.

### 2.6.4. Режим проверки примеров из списка образов

Быстрая проверка всех примеров из списка обучающих примеров осуществляется выбором подпункта "Проверить все образы из списка" пункта меню "Операции". При этом все примеры из списка последовательно подаются на обученную нейронную сеть, вычисляется выходной код и сравнивается с эталонным. На экран выводится отчёт об общем количестве проверенных примеров и количестве примеров, распознанных как "Свой" и "Чужой". Данный режим подходит для быстрой оценки качества обучения нейронной сети. Позволяет увидеть, все ли обучающие примеры правильно распознаются как "Свой". Если есть тестовые примеры образа "Свой", то можно увидеть какова ошибка первого рода, т.е. какой процент примеров правильно распознан как "Свой" и неправильно отнесён в группу "Чужой".

Также в режиме обучения можно активировать режим быстрой проверки примеров из списка обучающих примеров. Для активации режима проверки необходимо выбрать пункт меню "Операции", подпункт "Режим проверки" (рис. 23). Деактивация осуществляется аналогично.

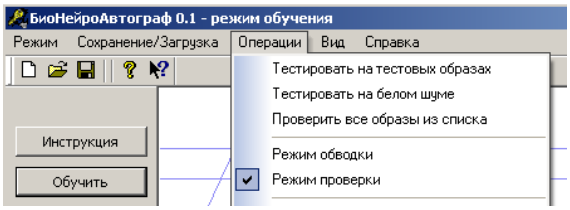



Рис. 23. Активация режима проверки

После активации в левом нижнем углу поля ввода рукописных образов появится красная надпись "Включён режим проверки". Теперь, если выбрать пример из списка, он будет автоматически подаваться на обученную нейронную сеть, вычисляться выходной код и сравниваться с эталонным, полученная мера Хемминга будет выводится в верхнем левом углу поля ввода.

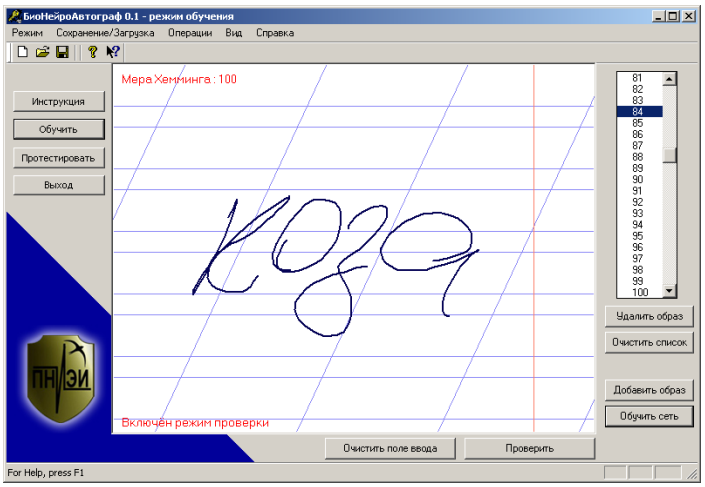



Рис. 24. Вычисление меры Хемминга образов в режиме проверки

Данный режим позволяет быстро вычислить меры Хемминга на всех примерах из списка, увидеть близкие и далёкие к обучающему примеру и оценить качество обучения нейронной сети.

### 2.7. Завершение работы

Окончание работы среды моделирования "БиоНейроАвтограф" осуществляется нажатием крестика в верхнем правом углу главного диалогового окна. При этом появляется диалоговое окно с предложение завершить или продолжить работу (рис. 24).

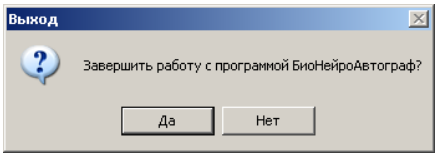



Рис. 25. Выход из программы

Для окончания работы необходимо нажать кнопку "Да".

Перед завершение работы необходимо сохранить обучающие примеры (если это необходимо). Все несохранённые данные после завершения работы приложения автоматически удаляются.

## 3. Пакет лабораторных работ по обучению и тестированию нейронной сети преобразователя биометрия-код

### 3.1. Работа №1 "Овладение технологией нейросетевого преобразования биометрических данных человека в код его личного ключа доступа или длинного пароля"

Основная проблема парольной защиты состоит в том, что обычные люди не способны помнить свой длинный пароль (ключ), если он сформирован по "правилам" и состоит из серии случайных символов и цифр. Так в среде моделирования "БиоНейроАвтограф" есть режим задания случайного пароля (рис. 26).

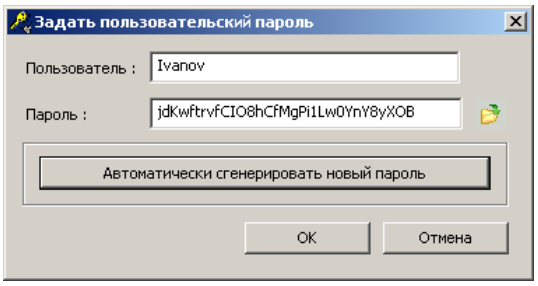



Рис. 26. Автоматическая генерация стойкого пароля

Попробуйте запомнить это число и воспроизвести его по памяти через пять минут. У вас это не получится, а вот воспроизвести своим рукописным почерком букву "*а*" для человека очень просто. Пароли и ключи нужны только машинам, для людей они неудобны. Нейросетевая биометрия как раз и нужна для того, чтобы облегчить людям запоминание длинных случайных паролей и криптографических ключей.

Целью лабораторной работы №1 является продемонстрировать студентам новые технологические возможности нейросетевого искусственного интеллекта биометрических приложений защиты информации.

Образец выполнения лабораторной работы №1 можно скачать с сайта ОАО "ПНИЭИ": http://пниэи.рф/activity/science/noc.htm.

### 3.2. Работа №2 "Оценка вероятности ошибок второго рода (пропуск "Чужого") по ГОСТ Р 52633.3, использующая статистики расстояний Хемминга"

При обычной обработке статистических данных оценивать вероятность появления редких событий очень утомительно. Для оценки вероятности события порядка 0,01 необходимо примерно 200 опытов. Для оценки вероятности 0.000001 нужно два миллиона опытов. Для того чтобы написать миллион рукописных слов (тетрадь рукописного текста в пять тысяч страниц, на каждой странице 200 слов) потребуется примерно полгода усилий.

Идти на такие затраты нет смысла, гораздо целесообразнее применить приём, изложенный в ГОСТ Р 52633.3 и перейти от статистической обработки обычных кодов к обработке расстояний Хемминга. Распределение расстояний Хемминга для кодов длиной 256 бит является нормальным при среднем модуле коэффициентов корреляции между разрядами менее 0.37. Если пользоваться гипотезой нормальности распределения расстояний Хемминга, то нет смысла ждать появления редких событий. Можно их предсказывать, вычислив математическое ожидание и среднеквадратическое отклонение расстояний Хемминга. Для достаточно точного вычисления математического ожидания и среднеквадратического отклонения достаточно всего 20 опытов. Подобная статистическая оценка легко осуществима силами студента за время, отведенное на одну лабораторную работу.

Целью лабораторной работы №2 является овладение студентами методом быстрого тестирования, рекомендуемого ГОСТ Р 52633.3

Образец выполнения лабораторной работы №2 можно скачать с сайта ОАО "ПНИЭИ": http://пниэи.рф/activity/science/noc.htm.

### 3.3. Работа №3 "Оценка вероятности ошибок первого рода (отказ в доступе "Своему"), использующая статистики расстояний Хемминга"

Нейросетевая биометрия может быть сделана высокодоступной, если того требует политика применения средства биометрической защиты. Обычно пользователей вполне устраивает вероятность ошибок первого рода (отказ "Своему") на уровне 0.1. Оценить такую вероятность можно, пользуясь 20 тестовыми образами "Свой", не участвовавшими в обучении искусственной нейронной сети.

Положение меняется, когда требуется обеспечить вероятность ошибок первого рода на уровне 0.001. В этом случае испытуемому потребуется предъявлять 2 000 своих рукописных образов при тестировании. Сократить объём тестовой выборки удаётся, если отказаться от привычного приёма фиксации нескольких редких событий. По аналогии с процедурой быстрого тестирования по ГОСТ Р 52633.3 следует перейти в пространство расстояний Хемминга между обучающим кодом "Свой" и кодами "Свой", полученными на 20 проверочных опытах.

Из теории известно, что сильно коррелированные коды "Свой" хорошо описываются хи-квадрат распределением с очень малым числом степеней свободы $m = E(h)$. Пользуясь этим правилом можно не ждать редких событий отказа "Своему" в доступе, а предсказывать вероятность появления этих редких событий.

Целью лабораторной работы №3 является познакомить студентов с алгоритмом ускоренного тестирования значения вероятности ошибок первого рода.

Образец выполнения лабораторной работы №3 можно скачать с сайта ОАО "ПНИЭИ": http://пниэи.рф/activity/science/noc.htm.

### 3.4. Работа №4 "Коррекция ошибок выходных кодов нейронной сети за счёт введения в эти коды избыточности"

Одним из путей повышения доступности средств биометрической аутентификации является коррекция небольшого числа ошибок в коде "Свой". Для этой цели можно использовать самокорректирующиеся избыточные коды.

Целью лабораторной работы №4 является демонстрация возможности применения для коррекции ошибок простейших приёмов, которые лежат в основе классических самокорректирующихся кодов.

К сожалению, среда моделирования "БиоНейроАвтограф" не способна продемонстрировать корректирующие возможности второго слоя нейронов, обученного по ГОСТ Р 52633.5. Сеть искусственных нейронов среды моделирования "БиоНейроАвтограф" однослойная. Убедиться в том, что нейросетевые корректоры ошибок кода намного эффективнее применения классических кодов нельзя. Этот тезис приходится принимать на веру, опираясь на логику. Логика сводится к тому, что все классические самокорректирующиеся коды синтезированы в рамках гипотезы о равновероятном распределении ошибок по разрядам выходного кода. Практика, наблюдаемая в лабораторной работе №4 иная, выходные коды имеют стабильные и нестабильные разряды. Нейросетевые корректоры эффективнее классических потому, что учитывают при обучении второго слоя нейронов собственные показатели стабильности каждого из разрядов выходного кода. Второй слой нейронной сети обладает большей информацией о корректируемом коде, чем любой из классических кодов, способных обнаруживать и корректировать ошибки.

Образец выполнения лабораторной работы №4 можно скачать с сайта ОАО "ПНИЭИ" http://пниэи.рф/activity/science/noc.htm.

### 3.5. Работа №5 "Оценка стойкости к атакам подбора частично и полностью скомпрометированного рукописного пароля"

Все биометрические технологии слабы. Сама биометрия даёт ошибку второго рода (пропуск "Чужого") на уровне 0.001. То есть около 2 000 попыток потребуется злоумышленнику на то, чтобы преодолеть любую биометрическую защиту. Однако столь неутешительные прогнозы распространяются только на ситуацию, когда злоумышленник знает биометрический образ атакуемого. Злоумышленник знает, что он должен создавать (воспроизводить, эмулировать). Если биометрический образ неизвестен, то стойкость к атакам биометрической защиты резко возрастает, биометрия становится высоконадёжной.

Целью лабораторной работы №5 является демонстрация студентам ослабления биометрической защиты при частичной и полной компрометации биометрического образа.

Образец выполнения лабораторной работы №5 можно скачать с сайта ОАО "ПНИЭИ" http://пниэи.рф/activity/science/noc.htm.

### 3.6. Работа №6 "Оценка достоверности гипотезы нормальности закона распределения расстояний Хемминга между кодами "Свой" и "Чужой"

Быстрое тестирование качества работы нейросетевых преобразователей биометрия-код по ГОСТ Р 52633.3 строится на гипотезе нормального распределения расстояний Хемминга между кодами "Свой" и кодами "все Чужие".

Целью лабораторной работы №6 является демонстрация студентам справедливости гипотезы нормальности закона распределения расстояний Хемминга.

По результатам лабораторной работы гипотеза нормальности должна выполняться с вероятностью 0.99987, 0.9999987, 0.99999987. Чем выше стойкость к атакам подбора

биометрического образа, тем больше должно быть девяток. При правильном выполнении работы число девяток вероятности выполнения гипотезы нормальности должно быть больше числа девяток вероятности ($1\text{-}P_2$). Разница обычно составляет от одной до трёх девяток, что и является численным подтверждением верности гипотезы о нормальном распределении значений.

Образец выполнения лабораторной работы №6 можно скачать с сайта ОАО "ПНИЭИ" http://пниэи.рф/activity/science/noc.htm.

### 3.7. Работа №7 "Тестирование стойкости к атакам подбора преобразователя биометрия-код на случайных и зависимых данных"

Подстановка многомерных случайных данных (белого шума) на вход нейронной сети – это самая бесполезная атака. Именно по этой причине она даёт сильно завышенную оценку стойкости преобразователя биометрия-код к атакам подбора. Криптографию можно ломать простым перебором всех возможных состояний ключа, для биометрии эта тактика неприемлема. Биометрию следует атаковать биометрическими образами, обладающими правдоподобными корреляционными матрицами. В этом случае оценка вероятности ошибок второго рода оказывается гораздо более правдоподобной.

Целью лабораторной работы №7 является демонстрация студентам низкой эффективности атак биометрии многомерным белым шумом.

Образец выполнения лабораторной работы №7 можно скачать с сайта ОАО "ПНИЭИ" http://пниэи.рф/activity/science/noc.htm.

### 3.8. Работа № 8 "Оценка достоверности гипотезы хи-квадрат распределения расстояний Хемминга между кодами "Свой" и "Свой"

Ускоренная оценка достигнутой вероятности ошибок первого рода (отказ в доступе "Своему") осуществляется в рамках гипотезы хи-квадрат распределения расстояний Хемминга между кодом "Свой", использованным при обучении и кодами "Свой", полученными в результате тестирования.

Для того чтобы убедиться в верности гипотезы нужно создать достаточно большую базу тестовых образов "Свой" и заведомо ухудшить обучение (недообучение или переобучение нейронной сети). Это позволяет построить гистограмму распределения расстояний Хемминга и сравнить её с эквивалентным хи-квадрат распределением.

По результатам лабораторной работы гипотеза хи-квадрат распределения должна выполняться с вероятностью 0.987, 0.9987. Чем выше доступность нейросетевого преобразователя, тем больше должно быть девяток. При правильном выполнении работы число девяток вероятности достоверности гипотезы хи-квадрат распределения должно быть больше числа девяток вероятности (1-P1). Разница обычно составляет примерно одну девятку, что и является численным подтверждением верности гипотезы о хи-квадрат распределении значений.

### 3.9. Работа №9 "Исследование эффектов от переобучения и недообучения искусственной нейронной сети"

Нейросетевые преобразователи биометрия-код учатся автоматами, выполненными по ГОСТ Р 52633.5. Однако эти автоматы не осуществляют оптимизацию числа примеров обучения "Свой". В результате при недостаточно количестве примеров образа "Свой" средство биометрической аутентификации оказывается недоученным (плохо узнаёт образ "Свой", но хорошо отсеивает образы "Чужой"). Если обучать на слишком большом количестве примеров образа "Свой", то средство биометрической аутентификации переучивается (хорошо узнаёт образы "Свой", но хуже отсеивает образы "Чужой").

Целью лабораторной работы №9 является обучение студентов поиску оптимального числа примеров в конкретной обучающей выборке, сформированной для оптимального обучения нейросетевого преобразователя биометрия-код.

### 3.10. Работа №10 "Исследование эффектов от появления грубых ошибок в обучающей выборке"

Грубые ошибки, иногда допускаемые пользователем, попав в обучающую выборку, приводят к значительному ухудшению качества обучения нейросетевого преобразователя.

Целью лабораторной работы №10 является демонстрация студентам влияния примеров с грубыми ошибками в обучающей выборке на качество обучения, выработка навыков выделения признаков грубых ошибок, которые позволяют исключить "ошибочные" примеры из обучающей выборки.

### 3.11. Работа №11 "Оценка коррелированности разрядов кодов "Свой" и "Чужой"

Из теории известно, что многомерная энтропия выходных кодов "Чужой" сильно зависит от коррелированности разрядов этих кодов. Зная энтропию кодов "Чужой" всегда можно вычислить среднее значение модулей корреляционных связей между разрядами кодов небелого шума.

Целью лабораторной работы №11 является оценка студентом влияния корреляционных связей между разрядами кодов "Чужой" на энтропию этих кодов и стойкость к атакам подбора нейросетевого преобразователя биометрия-код.

## 4. Калькулятор вычисления вероятности ошибок отказа "Своему"

В результате тестирования обученных нейросетевых преобразователей биометрия-код в рамках выполнения лабораторных работ №1,….,№11 студенты вычисляют статистики расстояний Хемминга. По полученным статистикам необходимо вычислить, соответствующую, вероятность появления ошибок первого рода (отказ "Своему"). Для этой цели разработан "Калькулятор $P_1$". Запуска калькулятора для вычисления вероятности появления ошибок первого рода необходимо запустить исполняемый файл CalculatorP1.exe, поставляемый совместно со средой моделирования "БиоНейроАвтограф". Главное диалоговое окно калькулятора представлено на рисунке 27.

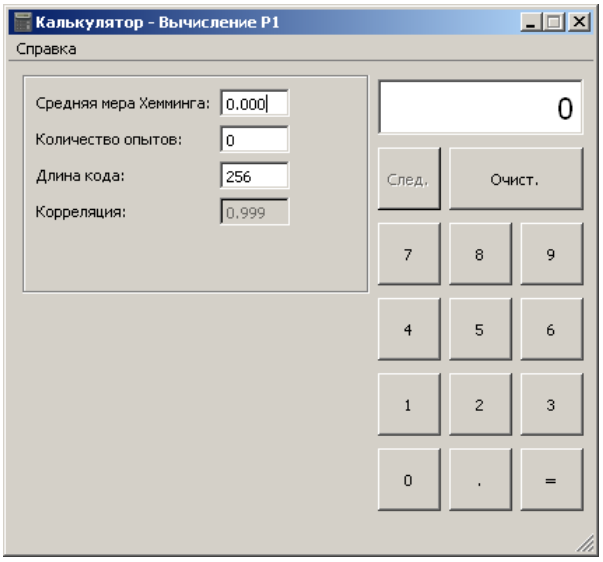



Рис. 27. Калькулятор вычисления ошибок первого рода

Для вычисления вероятности появления ошибки первого с помощью калькулятора необходимо в поле ввода "Средняя мера Хемминга" ввести значение средней меры Хемминга при тестировании обученной нейронной сети на тестовых образах "Свой". Если средняя мена Хемминга ненулевая, то поле "Количество опытов" можно оставить без изменения. Если значение средней меры Хемминга нулевое, то в поле "Количество опытов" нужно ввести число проведенных опытов. Если во время обучения использовался обучающий код длиной больше или меньше 256 бит, то необходимо заполнить поле "Длина кода".

После заполнения всех необходимых полей необходимо нажать кнопку "=" или клавишу "Enter" в поле ввода. Вычисленная вероятность ошибки первого рода выводится в поле вывода в правом верхнем углу диалогового окна.

## 5. Калькулятор вычисления вероятности ошибок пропуска "Чужого"

В результате тестирования обученных нейросетевых преобразователей биометрия-код в рамках выполнения лабораторных работ №1,….,№11 студенты вычисляют статистики расстояний Хэмминга. По этим статистикам необходимо вычислить, соответствующую, вероятность появления ошибок второго рода (пропуск "Чужого"). Для этой цели разработан "Калькулятор $P_2$". Запуска калькулятора для вычисления вероятности появления ошибок второго рода необходимо запустить исполняемый файл CalculatorP2.exe, поставляемый совместно со средой моделирования "БиоНейроАвтограф". Главное диалоговое окно калькулятора представлено на рисунке 28.

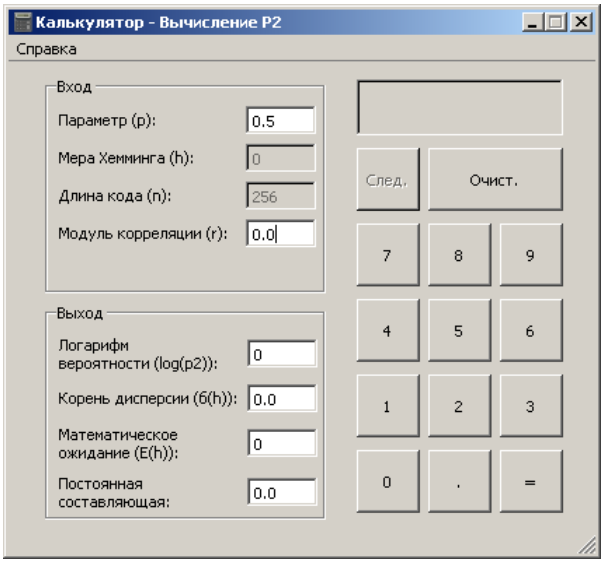



Рис. 28. Калькулятор вычисления ошибок второго рода

Пользоваться калькулятором можно задавая параметр симметрии – p (вероятность появления наиболее редких состояний "0" или "1" в разрядах анализируемых кодов "Чужой"). Так же необходимо задать среднее значение модулей корреляции – r. Тогда нажатие на кнопку "=" приводит к пересчету исходных данных в значения $\log_{10}(P_2)$, E(h) и б(h).

Можно поступать иначе, задавая E(h), б(h) и получая параметры $\log_{10}(P_2)$, p, r.

"Калькулятор $P_2$" осуществляет вычисления с приемлемой для инженерной практики точностью.

# ЛИТЕРАТУРА по нейросетевой биометрии

## 1. СТАНДАРТЫ


1.1 ГОСТ Р 52633.0-2006 "Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации".

1.2 ГОСТ Р 52633.1-2009 "Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации"

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

1.4 ГОСТ Р 52633.3-2011 "Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора".

1.5 ГОСТ Р 52633.4-2012 "Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код".

1.6 ГОСТ Р 52633.5-2011 "Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа".

1.7 ГОСТ Р 52633.6-2013 "Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу "Свой".

1.8 ГОСТ Р 52633.7-2013 "Защита информации. Техника защиты информации. Высоконадежная мультибиометрическая аутентификация"


## 2. КНИГИ


2.1 Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Изд-во Пенз. гос. ун-та, 2000. – 188 с.

2.2 Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности. Книга 15, серии "Нейрокомпьютеры и их применение" М.: Радиотехника 2004 г., 144 с.

2.3 Иванов А.И., Кисляев С.Е., Гелашвили П.А. Искусственные нейронные сети в биометрии, медицине, здравоохранении. Самара: ООО "Офорт", 2004, -236 с.

2.4 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.

2.5 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.

2.6 "Нейросетевое преобразование биометрического образа человека в код его личного криптографического ключа" Коллективная монография под редакцией А.Ю. Малыгина, Москва-2008 г, Радиотехника (ИПРЖ) книга №29 научной серии "Нейрокомпьютеры и их применение" 87 с.

2.7 Язов Ю.К. и др. Нейросетевая защита персональных биометрических данных. //Ю.К.Язов (редактор и автор), соавторы В.И. Волчихин, А.И. Иванов, В.А. Фунтиков, И.Г. Назаров // М.: Радиотехника, 2012 г. 157 с.