ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 52633.5— 2011

Защита информации

ТЕХНИКА ЗАЩИТЫ ИНФОРМАЦИИ

Автоматическое обучение нейросетевых преобразователей биометрия-код доступа

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России»), Федеральным государственным унитарным предприятием «Пензенский научно-исследовательский электротехнический институт» (ФГУП «ПНИЭИ»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 685-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ПЕРЕИЗДАНИЕ. Октябрь 2018 г.

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

© Стандартинформ, оформление, 2018

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Обозначения 5
5 Общие положения быстрого послойного обучения нейронных сетей преобразователей биометрия-код доступа 5
5.1 Классификация нейросетевых преобразователей биометрия-код доступа 5
5.2 Раздельное обучение каждого из нейронов нейросети 6
5.3 Раздельное обучение каждого из слоев нейронов нейросети 7
5.4 Контроль размеров и однородности примеров обучающей выборки образа «Свой» 7
5.5 Контроль размеров и независимости примеров обучающей выборки, представляющих хаос случайных образов «Все «Чужие» 8
6 Автомат обучения однослойной нейронной сети, работающей с непрерывными биометрическими данными низкого качества 8
6.1 Автоматический синтез связей первого слоя нейронов 8
6.2 Автоматическое обучение нейронов первого слоя 9
7 Автоматическое обучение нейронов второго слоя 11
7.1 Автоматический синтез связей нейронов второго слоя 11
7.2 Автоматическое обучение нейронов второго слоя 11
8 Использование автомата обучения второго слоя нейронов для обучения однослойной нейронной сети, ориентированной на работу с дискретными входными данными высокого качества 12
8.1 Нейросетевая корректировка дискретных входных биометрических данных с бинарными состояниями «0» и «1» в каждом разряде 12
8.2 Особенности нейросетевой корректировки дискретных входных биометрических данных с числом состояний более двух 12
9 Автоматическое прогнозирование качества обучения нейросетевого преобразователя биометрия-код доступа 13
9.1 Автоматическое прогнозирование стойкости к атакам подбора 13
9.2 Отображение результатов автоматического прогнозирования стойкости к атакам подбора . . . 13
9.3 Автоматическое прогнозирование вероятности ошибок первого рода обученного нейросетевого преобразователя биометрия-код доступа 13
9.4 Отображение результатов автоматического тестирования ошибок первого рода обученного нейросетевого преобразователя биометрия-код доступа 13
Приложение А (справочное) Примеры статистик распределения входных и выходных данных нейрона первого слоя на различных этапах обучения 14

Введение

Настоящий стандарт входит в комплекс стандартов, устанавливающих требования к разработке и тестированию средств высоконадежной биометрической аутентификации.

Важнейшим аспектом доверия к средствам высоконадежной биометрической аутентификации является то, насколько качественно обучен нейросетевой преобразователь биометрия-код доступа. Процесс обучения каждого искусственного нейрона преобразователя биометрия-код доступа должен быть полностью автоматизирован и обеспечивать высокий уровень вероятности принятия биометрического образа «Свой» при низком уровне вероятности ошибочного принятия биометрического образа «Чужой», оцениваемой по ГОСТ Р 52633.3.

Не все известные алгоритмы обучения искусственных нейронов могут быть применены при обучении средств высоконадежной биометрической аутентификации. Часть алгоритмов обучения искусственных нейронов неустойчива, и поэтому обучение с их помощью не может быть полностью автоматизировано. Другая часть алгоритмов обучения искусственных нейронов устойчива, но не дает необходимого качества обучения нейросетевого преобразователя биометрия-код доступа.

В настоящем стандарте описывается алгоритм обучения, который одновременно обладает высокой устойчивостью и обеспечивает достаточно высокое качество обучения с учетом специфических требований к нейросетевым преобразователям биометрия-код доступа, сформулированным в базовом стандарте ГОСТ Р 52633.0.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ТЕХНИКА ЗАЩИТЫ ИНФОРМАЦИИ

Автоматическое обучение нейросетевых преобразователей биометрия-код доступа

Information protection. Information protection technology.
The neural net biometry-code converter automatic training

Дата введения — 2012—04—01

1 Область применения

Настоящий стандарт распространяется на средства автоматического обучения нейросетевых преобразователей биометрия-код доступа, используемые при регистрации пользователей перед их высоконадежной биометрической аутентификацией по ГОСТ Р 52633.0. Во время своей регистрации пользователь предъявляет несколько примеров биометрического образа «Свой» и свой код доступа. Автомат обучения должен выполнить обучение нейросетевого преобразователя биометрия-код доступа так, чтобы при предъявлении преобразователю примеров образа «Свой» он выдавал на выходе код доступа «Свой», а при предъявлении преобразователю случайного образа «Чужой» преобразователь выдавал на выходе случайный код.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 19794-2—2005 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца — контрольные точки

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

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

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

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1

биометрические данные: Данные с выходов первичных измерительных преобразователей физических величин, совокупность которых образует биометрический образ конкретного человека.

[ГОСТ Р 52633.0—2006, пункт 3.5]

3.2

биометрический образ: Образ человека, полученный с выходов первичных измерительных преобразователей физических величин, подвергающийся далее масштабированию и иной первичной обработке с целью извлечения из него контролируемых биометрических параметров человека.

[ГОСТ Р 52633.0—2006, пункт 3.7]

3.3

преобразователь «биометрия-код»: Преобразователь, способный преобразовывать вектор нечетких, неоднозначных биометрических параметров «Свой» в четкий однозначный код ключа (пароля). Преобразователь, откликающийся случайным выходным кодом на воздействие случайного входного вектора, не принадлежащего множеству образов «Свой».

[ГОСТ Р 52633.0—2006, пункт 3.18]

3.4

естественный биометрический образ: Биометрический образ донора, полученный в виде выходных биометрических данных первичного преобразователя и представленный одним или несколькими примерами.

[ГОСТ Р 52633.1—2009, пункт 3.3]

3.5

синтетический биометрический образ: Биометрический образ, полученный путем имитационного моделирования естественных биометрических образов и представленный одним или несколькими примерами.

[ГОСТ Р 52633.1—2009, пункт 3.4]

3.6

база естественных биометрических образов «Чужой»: Совокупность естественных биометрических образов, имитирующих предъявляемые средству аутентификации злоумышленником (злоумышленниками) случайные биометрические образы при реализации атаки подбора.

[ГОСТ Р 52633.1—2009, пункт 3.5]

3.7

база естественных биометрических образов «Свой»: Совокупность естественных биометрических образов, состоящая из нескольких примеров одних и тех же биометрических образов, предназначенных для обучения или тестирования средств биометрической аутентификации.

[ГОСТ Р 52633.1—2009, пункт 3.6]

3.8

критерий Хемминга: Мера сравнения двух кодов одинаковой длины, вычисляемая путем подсчета различающихся разрядов сравниваемых кодов.

[ГОСТ Р 52633.1—2009, пункт 3.16]

3.9

показатель стабильности биометрического параметра: Характеристика *i*-го контролируемого биометрического параметра, вычисляемая по формуле

$$c(v_i) = \frac{\sigma_{\text{Чужой}}(v_i)}{\sigma_{\text{Свой}}(v_i)},$$

где $\sigma_{\text{Чужой}}(v_i)$ — стандартное отклонение *i*-го биометрического параметра множества образов «Чужой»

$\sigma_{\text{Свой}}(v_i)$ — стандартное отклонение *i*-го биометрического параметра множества образов «Свой».

[ГОСТ Р 52633.1—2009, пункт 3.7]

3.10

показатель уникальности биометрического параметра: Характеристика *i*-го биометрического параметра, отражающая отличие контролируемого параметра от среднестатистического значения этого параметра, характерного для всех пользователей, вычисляемый по формуле

$$u(v_i) = \frac{|E_{\text{Чужой}}(v_i) - E_{\text{Свой}}(v_i)|}{\sigma_{\text{Чужой}}(v_i)},$$

где $E_{\text{Чужой}}(v_i)$ — математическое ожидание *i*-го биометрического параметра множества биометрических образов «Чужой»;

$E_{\text{Свой}}(v_i)$ — математическое ожидание *i*-го биометрического параметра множества биометрических образов «Свой»

[ГОСТ Р 52633.1—2009, пункт 3.9]

3.11

показатель качества биометрического параметра: Характеристика *i*-го биометрического параметра, вычисляемая по формуле

$$q(v_i) = \frac{|E_{\text{Чужой}}(v_i) - E_{\text{Свой}}(v_i)|}{\sigma_{\text{Чужой}}(v_i) + \sigma_{\text{Свой}}(v_i)}$$

[ГОСТ Р 52633.1—2009, пункт 3.11]

3.12

биометрический пример: Совокупность биометрических данных, полученная с выхода первичного преобразователя при однократном предъявлении человеком своего биометрического образа.

[ГОСТ Р 52633.2—2010, пункт 3.12]

3.13

морфинг биометрических примеров: Создание промежуточного синтетического биометрического образа(ов), основанное на нахождении некоторого промежуточного значения каждого из биометрических параметров пары биометрических образов-родителей.

[ГОСТ Р 52633.2—2010, пункт 3.14]

3.14

биометрический пример-родитель: Биометрический пример, используемый для создания биометрических примеров-потомков в процессе морфинга примеров биометрических образов.

[ГОСТ Р 52633.2—2010, пункт 3.16]

3.15

биометрический пример-потомок: Биометрический пример, создаваемый в процессе морфинга пары биометрических примеров-родителей.

[ГОСТ Р 52633.2—2010, пункт 3.18]

3.16

дискретный биометрический параметр: Биометрический параметр, значения которого составляют конечное множество.

[ГОСТ Р 52633.4—2011, пункт 3.11]

3.17

непрерывный биометрический параметр: Биометрический параметр, значения которого составляют континуальное множество.

[ГОСТ Р 52633.4—2011, пункт 3.12]

3.18

вектор биометрических параметров; ВБП: Нумерованный набор биометрических параметров или производных от них параметров, имеющих одну и ту же интерпретацию и формой представления.

[ГОСТ Р 52633.4—2011, пункт 3.13]

3.19

выходной код: Код, получаемый на выходе преобразователя биометрия-код в качестве результата.

[ГОСТ Р 52633.4—2011, пункт 3.14]

3.20

нейросетевой биометрический контейнер; НБК: Структурированный блок данных, содержащий параметры обученного НПБК.

[ГОСТ Р 52633.4—2011, пункт 3.22]

3.21

защищенный нейросетевой биометрический контейнер: Нейросетевой биометрический контейнер, в котором некоторые части скрыты от непосредственного изучения путем использования обратимого или необратимого преобразования.

[ГОСТ Р 52633.4—2011, пункт 3.23]

3.22 **весовой коэффициент входа нейрона:** Коэффициент, взвешивающий биометрические данные, поступающие на один из входов сумматора нейрона.

3.23 **нейрон:** Сумматор нескольких биометрических параметров, на выходе которого подключена нелинейная пороговая функция с двумя выходными состояниями «0» и «1».

3.24 **нейронная сеть:** Множество нейронов, объединенных в сеть путем соединения входов нейронов одного слоя с выходами нейронов другого слоя, причем, входы нейронов первого слоя являются входами всей нейронной сети, а выходы нейронов последнего слоя являются выходами нейронной сети.

Примечание — Настоящий стандарт в преобразователях биометрия-код доступа рекомендует использовать однослойные или двухслойные нейронные сети. Нейронные сети с большим числом слоев в настоящем стандарте не рассматриваются.

3.25 **показатель стабильности разряда выходного кода:** Показатель, изменяющийся в пределах от 0,0 (разряд абсолютно нестабилен) до 1,0 (разряд полностью стабилен), вычисляемый по формуле

$$\omega_j = 2|0{,}5 - P_{0,j}| = 2|0{,}5 - P_{1,j}|, \qquad (1)$$

где $P_{0,i}$ — вероятность появления состояния «0» в контролируемом i-ом разряде;

$P_{1,i}$ — вероятность появления состояния «1» в контролируемом i-ом разряде.

Примечание — Для образов «Свой» разряды выходного кода обычно стабильны, то есть для них выполняется условие $0,5 < \omega_i < L$ 1,0, а для образов «Чужой» большинство разрядов выходного кода нестабильны, то есть для них выполняется условие $0,0 \le \omega_i \le 0,5$.

3.26 **обучение нейрона:** Операция по вычислению либо подбору весовых коэффициентов нейрона, обеспечивающая высокую вероятность заранее заданного выходного состояния нейрона («0» или «1») при воздействии на него примерами образа «Свой» и равновероятные выходные состояния («0» и «1») при воздействии на нейрон примерами случайных образов «Чужой».

4 Обозначения

В настоящем стандарте использованы следующие обозначения:

N_0 — число входов всей нейронной сети;

N_1 — число нейронов первого слоя нейросети (число выходов нейронов первого слоя);

N_2 — число нейронов второго слоя нейросети (число выходов нейронов второго слоя);

μ — весовой коэффициент сумматора нейрона,

N — число входов одного обучаемого нейрона, используемого для обработки биометрических данных;

v — входные данные обучаемого нейрона;

y — выходные данные сумматора обучаемого нейрона;

ω — показатель стабильности разряда кода «Свой» на выходе нейрона первого слоя;

$E(.)$ — оператор вычисления математического ожидания;

$\sigma(.)$ — оператор вычисления стандартного отклонения;

P_1 — вероятность ошибки первого рода (ошибочный отказ «Своему»).

5 Общие положения быстрого послойного обучения нейронных сетей преобразователей биометрия-код доступа

5.1 Классификация нейросетевых преобразователей биометрия-код доступа

5.1.1 Нейросетевые преобразователи биометрия-код доступа классифицируют по виду входных биометрических параметров следующим образом:

- нейросетевые преобразователи, ориентированные на работу с непрерывными биометрическими параметрами, имеющими, как правило, низкое среднее входное качество;
- нейросетевые преобразователи, ориентированные на работу с дискретными биометрическими параметрами, имеющими, как правило, хорошее среднее входное качество.

Специализация нейронных сетей на обработку непрерывных или дискретных биометрических параметров обусловлена значительным различием алгоритмов их обучения и автоматов, реализующих эти алгоритмы.

5.1.2 Нейросетевые преобразователи биометрия-код доступа классифицируют по числу слоев нейронов, содержащихся в их нейронной сети. Различают нейросетевые преобразователи:

- с однослойной нейронной сетью;
- с двухслойной нейронной сетью.

Двухслойные нейронные сети, как правило, способны решать любые задачи высоконадежной биометрической идентификации и аутентификации. Дальнейшее увеличение числа слоев возможно, но для большинства биометрических приложений является избыточным и не рассматривается в рамках настоящего стандарта.

Нейронные сети должны осуществлять обогащение (повышение качества) исходных биометрических данных. Если удается решить задачу повышения качества исходных биометрических данных до приемлемого качества однослойной нейронной сетью, то применение для решения той же задачи двухслойной нейронной сети не рекомендуется. Корректировка незначительного числа ошибок однослойной нейронной сети допускается классическим избыточным кодом с обнаружением и исправлением ошибок.

5.2 Раздельное обучение каждого из нейронов нейросети

Процедура обучения нейронной сети преобразователя биометрия-код доступа является опасной, так как опирается на использование примеров образа «Свой» и знание кода доступа (возможна компрометация этих данных). В связи с этим обучение должно проводиться: в доверенной вычислительной среде, в автоматическом режиме, при минимальных затратах времени, под контролем донора биометрии «Свой». Сокращение времени обучения следует осуществлять за счет независимого обучения каждого из нейронов сети и отказа от многократного применения итерационных процедур подбора весовых коэффициентов нейрона. Блок-схема обучения одного искусственного нейрона представлена на рисунке 1.

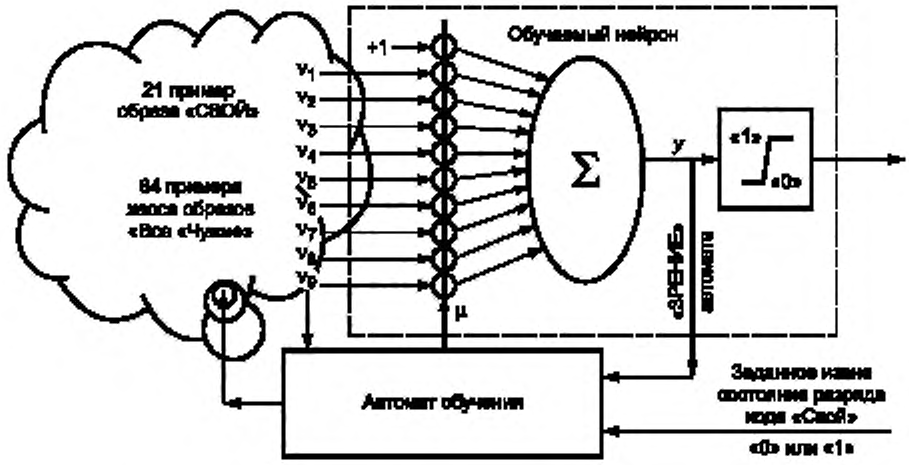

Рисунок 1 — Блок-схема обучения одного искусственного нейрона

В однослойных нейронных сетях один нейрон отвечает за один разряд выходного кода. Задачей автомата обучения является поиск (вычисление) таких весовых коэффициентов нейрона μ_i, которые смещают распределение откликов сумматора нейрона в заданное извне состояние его выходной нелинейности («0» или «1»). Пример распределения откликов нейрона на образ «Свой» до и после обучения приведен на рисунке 2.

Обучающий автомат должен наблюдать входные биометрические данные нейрона, относящиеся к примерам образа «Свой» и относящиеся к примерам случайных образов «Чужие». Автомат обучения видит отклики на выходе сумматора нейрона (до их искажения нелинейным элементом нейрона).

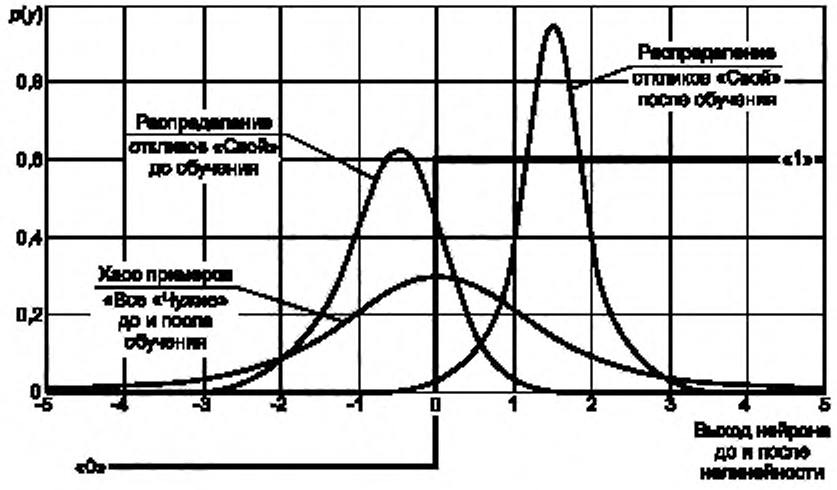

Рисунок 2 — Пример распределения откликов «Свой» и «Чужой» на выходе нейрона до и после его обучения

Фактически автомат обучения одного нейрона должен решать задачу выталкивания распределения откликов нейрона на примеры образа «Свой» на периферию распределения откликов образов «Чужой». Выталкивание необходимо осуществлять вычислением почти всех (кроме одного — μ_0) весовых коэффициентов связей нейрона. Нулевой коэффициент нейрона μ_0 необходимо использовать для приведения точки переключения нелинейной функции в точку, соответствующую математическому ожиданию примеров образов «Все «Чужие», для выполнения требования ГОСТ Р 52633.0 по равновероятному состоянию «0» и «1» выхода нейрона для образов «Чужие».

Примечание — Выталкивание на периферию распределения «Чужой» откликов «Свой» может осуществляться автоматом обучения в любом направлении (как в правую, так и в левую сторону (см. рисунок 2). Для того, чтобы изменить выходной код отклика «Свой», достаточно сменить знаки всех весовых коэффициентов, начиная с μ_1 до μ_n, что позволяет перепрограммировать код доступа без последующего переобучения нейронов и всей нейронной сети.

5.3 Раздельное обучение каждого из слоев нейронов нейросети

В простейшем случае однослойной нейронной сети обучение нейронов должно осуществляться поочередно, в порядке увеличения номера нейрона в слое.

В случае обучения двухслойной нейронной сети обучение следует вести, начиная с нейронов первого слоя. После обучения всех нейронов первого слоя следует осуществлять трансляцию примеров образа «Свой» и примеров образов «Чужие» со входов первого слоя на его выходы. Далее необходимо приступить к обучению второго слоя нейронов. Для этого следует использовать ранее полученные данные примеров «Свой» и «Чужой» на выходах первого слоя нейронов.

Обучение каждого слоя нейронов следует вести своим автоматом, учитывающим особенности той или иной биометрической технологии при входных данных разного качества. При обучении каждого слоя нейронов необходимо использовать свой выходной код. Выходной код промежуточного слоя должен быть получен от генератора случайных чисел. Все выходные коды обучения (код первого слоя и код второго слоя) должны быть уничтожены после обучения нейронной сети и проверки качества обучения.

5.4 Контроль размеров и однородности примеров обучающей выборки образа «Свой»

5.4.1 Размер обучающей выборки примеров «Свой»

При обучении необходимо использовать не менее 11 примеров образа «Свой». После обучения нейронной сети следует контролировать качество обучения не менее чем на трех примерах, не участвовавших в обучении. При выявлении отказа в доступе не прошедший распознавание пример следу-

ет добавить в обучающую выборку. Увеличение обучающей выборки необходимо вести до устойчивого узнавания «Своего» в трех-четырех следующих подряд попытках.

Рекомендуется дообучение средства высоконадежной аутентификации на примерах биометрического образа «Свой», предъявленных пользователем через несколько часов (несколько дней) после первоначального обучения.

При необходимости последующего дообучения средства (переобучения средства) базу примеров образа «Свой» следует хранить в доверенной вычислительной среде. Если хранение базы осуществляется в недоверенной вычислительной среде, то необходима защита базы обучения от ее компрометации.

5.4.2 Контроль однородности обучающей выборки

Перед каждым обучением (дообучением) средства аутентификации необходимо проверить однородность обучающей выборки. Для этой цели следует вычислить математическое ожидание каждого из контролируемых биометрических параметров и относительно него вычислить значение χ^2 — отклонение от центра биометрического образа «Свой» (от математического ожидания образа «Свой» по каждому из контролируемых параметров).

Примеры «Свой», значительно превышающие среднеквадратическое отклонение по критерию χ^2, необходимо удалить из обучающей выборки как грубую ошибку. Допускается проведение проверки по входным данным нейронной сети, а также проверки по выходным откликам сумматоров уже обученной нейронной сети.

5.5 Контроль размеров и независимости примеров обучающей выборки, представляющих хаос случайных образов «Все «Чужие»

Для обучения преобразователя биометрия-код доступа необходимо иметь не менее 64 примеров различных случайных (независимых) естественных биометрических образов «Чужие».

Контроль уровня взаимной независимости образов «Чужой» следует осуществлять взаимным сравнением их кодов на выходе одного ранее обученного однослойного преобразователя биометрия-код доступа, не имеющего механизма защиты от наблюдения внутренних данных. В обучающей выборке не должно быть пар биометрических образов, чьи выходные коды по критерию Хемминга выпадают из интервала

$$\left[\frac{N-2\sqrt{N}}{2}, \frac{N+2\sqrt{N}}{2}\right],$$

где N — число разрядов в выходном коде обучаемого нейросетевого преобразователя.

6 Автомат обучения однослойной нейронной сети, работающей с непрерывными биометрическими данными низкого качества

6.1 Автоматический синтез связей первого слоя нейронов

6.1.1 Прогнозирование необходимого числа входов одного нейрона

Прогнозирование необходимого числа входов одного нейрона следует осуществлять через задание желаемого выходного качества обученного нейрона $Q(y)$ на выходе сумматора нейрона y, которое в иных случаях следует вычислять по формуле

$$Q(y) = \frac{|E_{\text{Чужой}}(y) - E_{\text{Свой}}(y)|}{\sigma_{\text{Свой}}(y)}. \qquad (2)$$

Число входов y нейрона необходимо вычислять по формуле

$$n \approx a_0 \left\{\frac{Q(y)}{E(Q(v_i))}\right\}^2, \qquad (3)$$

где a_0 — нормирующий коэффициент, экспериментально подбираемый для автомата обучения при разработке средства биометрической аутентификации под каждую биометрическую технологию и для каждого слоя нейронов;

$Q(v_i)$ — псевдодискретное входное качество i-го входного биометрического параметра нейрона, вычисляемое по формуле

$$Q(v_i) = \frac{|E_{\text{Чужой}}(v_i) - E_{\text{Свой}}(v_i)|}{\sigma_{\text{Свой}}(v_i)}, \quad (4)$$

Примечание — Вместо задания желаемого качества обучения нейрона $Q(y)$ допускается задавать желаемое значение вероятности появления ошибок первого рода P_1, обученного нейрона. В этом случае качество обучения следует найти путем решения следующего уравнения:

$$P_1 \approx \left\langle \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \cdot \int_0^{a_1 Q(y)} \exp\left(-\frac{t^2}{2}\right) dt \right\rangle = \frac{1}{2} - \Phi_0(a_1 Q(y)), \quad (5)$$

где a_1 — нормирующий коэффициент, экспериментально подбираемый для автомата обучения при разработке средства биометрической аутентификации под каждую биометрическую технологию и для каждого слоя нейронов.

6.1.2 Выбор числа нейронов в первом слое нейронной сети

Число нейронов в первом слое нейронной сети N_1 следует задавать равным длине выходного кода доступа, если ошибки первого рода обученного слоя нейронов оказываются меньше желаемой вероятности ошибки первого рода всего средства аутентификации. Если вероятность ошибки первого рода оказывается равной или больше желаемой, то необходимо увеличить число нейронов в слое на число избыточных разрядов кода, способного обнаруживать и исправлять ошибки. При принятии решения об использовании того или иного классического кода, способного исправлять ошибки нейронов первого слоя, полностью снимается неопределенность относительно его избыточности.

Примечание — Первый слой нейронов осуществляет обогащение относительно бедных входных биометрических данных, в связи с этим число используемых входов нейросети N_0 берут значительно больше, чем число нейронов N_1, содержит обучаемый слой нейросети. Чем хуже входные биометрические данные, тем больше их потребуется для обогащения.

6.1.3 Автоматическое распределение связей входов нейронов с младшими адресами

Распределение адресов связей младших входов нейронов с входными данными всей нейронной сети должно осуществляться автоматически. Для первых $k = N_0/n$ нейронов следует выбирать входные связи с номерами от 1 до n, далее с номерами от $n + 1$ до $2n$. Соответственно входные связи k-го нейрона должны быть соединены со входами всей нейронной сети, имеющими номера от $(k - 1)n + 1$ до kn. Остаток незадействованных входов $(N_0 - kn)$ необходимо использовать для формирования связей последующих $(N_1 - k)$ нейронов первого слоя.

6.1.4 Автоматическое распределение связей входов нейронов со старшими адресами

Оставшиеся $(N_1 - k)$ нейронов первого слоя следует подключать к входам нейронной сети случайно, причем автомат, осуществляющий подключения, должен одновременно с подключением входов контролировать частоту использования всех входов. Автомат формирования случайных связей должен отключать слишком часто используемые входные данные и увеличивать число подключений редко используемых данных. Выравнивание частот подключения должно осуществляться до момента, пока минимальная частота использования входов нейросети не будет отличаться от максимальной частоты на две единицы.

После формирования случайных связей первого слоя нейронов необходимо осуществлять выявление и уничтожение общих связей в двух, трех, четырех нейронах с рядом лежащими номерами.

6.2 Автоматическое обучение нейронов первого слоя

6.2.1 Автоматическое обучение нейрона со статистическим вычислением весовых коэффициентов

Автоматы для реализации быстрых алгоритмов обучения нейронов должны задавать значения весовых коэффициентов μ_i равными нормированному псевдодискретному входному качеству по формуле (3), соответствующего биометрического параметра:

$$\mu_i = \frac{Q(v_i)}{\sigma_{\text{Чужой}}(v_i)}. \quad (6)$$

6.2.2 Присвоение знака вычисленным весовым коэффициентам

Знак при весовом коэффициенте следует задавать исходя из знака математического ожидания, учитываемого биометрического параметра и заданного при обучении состояния выхода нейрона. Для сумматора без инверсии блок-схемы (см. рисунок 2) при требуемом состоянии «1» кода «Свой» на выходе нейрона знак весового коэффициента μ_i должен совпадать со знаком разницы математических ожиданий образов «Свой» и «Чужой». Для обеспечения состояния «0» на выходе нейрона необходима инверсия разницы упомянутых выше математических ожиданий или

$$\begin{cases} \text{если «Свой»} \rightarrow \text{«1»}, \text{ то } sign(\mu_i) = sign\,(E_{\text{Свой}}(v_i) - E_{\text{Чужой}}(v_i)); \\ \text{если «Свой»} \rightarrow \text{«0»}, \text{ то } sign(\mu_i) = -\,sign\,(E_{\text{Свой}}(v_i) - E_{\text{Чужой}}(v_i)), \end{cases} \quad (7)$$

при условии, что нелинейный элемент нейрона принимает состояние «1» при положительных входных воздействиях и состояние «0» при отрицательных входных воздействиях.

6.2.3 Проверка достигнутого качества обучения

После вычисления весовых коэффициентов нейронов с номерами $i = 1, 2, 3, \ldots n$ необходимо осуществить вычисление нулевых весовых коэффициентов μ_0. Далее следует провести тестовую оценку достигнутого качества обучения по формуле (2) или оценку вероятности ошибок второго рода. Если показатели качества обучения нейрона достаточно высоки, то обучение следует прекратить. Если показатели качества обучения нейрона оказываются хуже порога, заложенного в автомат обучения, то автомат обучения должен увеличить число входов у нейрона и вычислить для них весовые коэффициенты. Увеличение числа входов нейрона следует проводить до момента, когда качество обучения окажется выше заданного автомату обучения порога.

6.2.4 Проверка уровня корреляционных связей обученных нейронов

Случайно выбранные пары нейронов, находящиеся в одном слое, имеют общие входы и, соответственно, выходные отклики нейронов имеют корреляционные связи. Для контроля уровня корреляционных связей следует выполнить их вычисление при воздействии на нейронную сеть не менее 10 000 случайных независимых входных воздействий с нормальным законом распределения значений, имеющим среднеквадратическое отклонение, равное среднеквадратическому отклонению биометрических параметров образов «Чужой». Данные тестирования следует получать от генератора случайных или псевдослучайных чисел.

При вычислениях необходимо использовать проверку не менее 128 случайно выбранных пар нейронов. Для каждой пары нейронов при вычислениях следует использовать выходы их сумматоров и далее следует вычислять математическое ожидание модуля полученных коэффициентов корреляции.

6.2.5 Маскирование корреляционных связей обученного нейрона

Для исключения возможности атаки на преобразователь биометрия-код доступа через вычисление коэффициентов корреляции у обученного нейрона следует изменить часть знаков весовых коэффициентов на противоположные. Часть измененных знаков по отношению к оставшейся части знаков весовых коэффициентов должна быть больше, чем среднее значение модуля корреляционных связей между парами нейронов, вычисленных по 6.2.4. Выбор изменяемых знаков необходимо осуществлять случайно.

Примечание — Изменение знака части связей нейрона на противоположные лишает атакующего уверенности в том, что он верно наблюдает коэффициенты корреляции. Включение механизма размножения ошибок мешает атакующему верно видеть корреляции между выходами нейронов. Чем выше качество механизма размножения ошибок, тем у меньшей части весовых коэффициентов следует искажать знаки.

6.2.6 Повторная проверка качества обучения нейронов

Маскирование корреляционных связей обученного нейрона по 6.2.5 обычно приводит к значительному снижению среднего качества обучения нейронов. Соответственно необходимо осуществить повторный контроль остаточного качества обучения.

Если остаточное качество обучения оказывается приемлемым, то нет смысла использовать второй слой нейронов.

При недостаточном качестве принятия решений первым слоем нейронов необходимо использовать второй слой нейронов.

7 Автоматическое обучение нейронов второго слоя

7.1 Автоматический синтез связей нейронов второго слоя

7.1.1 Задачи, выполняемые вторым слоем нейронов

Основной задачей нейронов второго слоя является повышение качества решений, принятых нейронами первого слоя в части снижения P_1 — вероятности ошибок первого рода. Второй слой нейронов выполняет функцию избыточных кодов с обнаружением и исправлением ошибок и, соответственно число выходов нейронов первого слоя N_1 может быть увеличено по 6.1.2.

Основное отличие нейросетевого корректирования ошибок от использования классических кодов с обнаружением и исправлением ошибок в их меньшей избыточности. Исправление ошибок, осуществляемое нейронами второго слоя, при одинаковой избыточности обеспечивает более высокий уровень числа исправленных ошибок, так как при обучении нейронов второго слоя автоматически учитывается положение стабильных и нестабильных разрядов в корректируемом коде, а так же уровень стабильности того или иного нестабильного разряда кода первого слоя нейронов.

7.1.2 Входные данные нейронов второго слоя

В случае использования двухслойной нейронной сети состояния разрядов выходного кода первого слоя должны быть изменены. Необходимо перейти от промежуточных кодов с состояниями разрядов «0» и «1» к эквивалентным кодам с состояниями «–1» и «+1».

7.1.3 Выбор числа нейронов второго слоя

Выбор числа нейронов второго слоя полностью повторяет процедуру выбора числа нейронов первого слоя по 6.1.2.

7.1.4 Выбор числа входов нейронов второго слоя

Число входов нейронов второго слоя необходимо выбирать в интервале от 0,2 N_1 до 0,8N_1 в зависимости от числа допускаемых ошибок кода нейронов первого слоя. Связь числа входов у нейронов второго слоя с числом ошибок нейронов первого слоя для образа «Свой» задается таблицами, а значения данных в таблицах подбирают экспериментально при разработке средства высоконадежной биометрической аутентификации.

7.1.5 Автоматическое распределение адресов связей нейронов второго слоя

Адреса связей нейронов второго слоя с выходами нейронов первого слоя выбираются случайно. При этом необходимо контролировать отсутствие повторений связей у каждого из нейронов, а также добиваться равной частоты использования каждого из выходов нейронов предыдущего слоя.

7.2 Автоматическое обучение нейронов второго слоя

7.2.1 Вычисление модулей весовых коэффициентов обучаемого нейрона

Модули весовых коэффициентов обучаемого нейрона μ_i вычисляют по формуле

$$\mu_i = \frac{a_2 \cdot \omega_i}{E(\omega_i)}, \tag{8}$$

где a_2 — стабилизирующий коэффициент, экспериментально подбираемый для автомата обучения при разработке средства биометрической аутентификации под каждую биометрическую технологию;

ω_i — показатель стабильности i-го разряда выходного кода нейронов первого слоя.

7.2.2 Случайная подстановка знаков весовых коэффициентов

Перед процедурой обучения необходимо осуществить случайную подстановку знаков весовых коэффициентов нейрона. После получения случайной последовательности знаков необходимо провести проверку баланса числа положительных и отрицательных знаков на входах обучаемого нейрона.

Если у обучаемого нейрона четное число входов, то число положительных и отрицательных знаков весовых коэффициентов нейрона должно быть одинаковым. Балансировка по знакам осуществляется исправлением избыточных знаков на инверсные.

Если у обучаемого нейрона нечетное число входов, то число положительных и отрицательных знаков весовых коэффициентов нейрона должно отличаться на единицу. Балансировка по знакам осуществляется исправлением избыточных знаков на инверсные.

7.2.3 Установка начальных условий обучения нейрона

После случайной установки знаков весовых коэффициентов проводят проверку наиболее вероятного выходного состояния обучаемого нейрона.

Если наиболее вероятное выходное состояние обучаемого нейрона совпадает с заданным выходным состоянием разряда выходного кода, то все знаки весовых коэффициентов инвертируют.

Если наиболее вероятное выходное состояние обучаемого нейрона не совпадает с заданным выходным состоянием разряда выходного кода, то все знаки весовых коэффициентов оставляют без изменений.

7.2.4 Обучающая корректировка знаков весовых коэффициентов

Обучение проводят путем корректировки знаков весовых коэффициентов у части входов нейрона. Корректировку знака выполняют так, чтобы вероятность появления заданного отклика на выходе нейрона при предъявлении примеров образа «Свой» увеличивалась (число ошибок выходного кода уменьшалось).

Корректировку проводят по одному входу. Если смена знака весового коэффициента корректируемого входа дает обратный результат, то корректировку следует отменить и перейти к корректировке знака следующего весового коэффициента.

Корректировку знаков весовых коэффициентов проводят до момента, пока не будут устранены все ошибки в кодах первого слоя нейрона, возникающие при воздействии на обучаемую нейронную сеть всеми обучающими примерами образов «Свой».

8 Использование автомата обучения второго слоя нейронов для обучения однослойной нейронной сети, ориентированной на работу с дискретными входными данными высокого качества

8.1 Нейросетевая корректировка дискретных входных биометрических данных с бинарными состояниями «0» и «1» в каждом разряде

В ряде приложений биометрические данные являются изначально дискретными и имеют высокое входное качество (например, данные о существовании или отсутствии особых точек в контролируемой области рисунка отпечатка пальца). В этом случае нейронная сеть должна работать с входными дискретными биометрическими данными, имеющими два состояния: «0» — нет особенностей, «1» — особенность обнаружена, то есть второй слой обычной нейронной сети, ориентированный на работу с дискретными данными первого слоя может быть использован самостоятельно как однослойная сеть нейронов. В этом случае обучение первого слоя сети нейронов, работающих с дискретными данными, совпадает с обучением второго слоя, в соответствии с разделом 7.

8.2 Особенности нейросетевой корректировки дискретных входных биометрических данных с числом состояний более двух

В ряде случаев число состояний дискретных биометрических параметров может быть более двух. В этих случаях необходима перекодировка дискретных параметров. В нейросетевых преобразователях следует использовать новый бинарный код с длиной кода, равной числу состояний биометрического параметра, и единственным разрядом, имеющим состояние «1».

Примечание — По ГОСТ Р ИСО/МЭК 19794-2 рисунок отпечатка пальца имеет три типа состояний контрольных областей (биометрических параметров), кодирующихся как:

«00» — область, где нет особенностей;

«01» — область, где есть точка окончания гребня;

«10» — область, где есть точка бифуркации гребня.

В этом случае при кодировании состояний областей с особыми точками рисунка отпечатка пальца для нейросетевого преобразователя следует использовать другие коды входных состояний:

«100» — область, в которой нет особенностей;

«010» — область, в которой есть точка окончания гребня;

«001» — область, в которой есть точка бифуркации гребня.

9 Автоматическое прогнозирование качества обучения нейросетевого преобразователя биометрия-код доступа

9.1 Автоматическое прогнозирование стойкости к атакам подбора

После обучения нейросетевого преобразователя биометрия-код доступа (однослойного или двухслойного) необходимо осуществить прогнозирование его стойкости к атакам подбора согласно 6.3 ГОСТ Р 52633.0—2006. Прогнозирование необходимо осуществлять в соответствии с разделами 5 и 6 ГОСТ Р 52633.3—2011.

9.2 Отображение результатов автоматического прогнозирования стойкости к атакам подбора

Отображение результатов автоматического прогнозирования стойкости к атакам подбора для обученного нейросетевого преобразователя биометрия-код доступа должно осуществляться с учетом классификации биометрического образа по его средней стабильности, средней уникальности, среднему качеству параметров. Интерфейс отображения должен показывать пользователю, насколько параметры его биометрического образа отличаются от параметров среднестатистического пользователя в сторону улучшения или ухудшения.

9.3 Автоматическое прогнозирование вероятности ошибок первого рода обученного нейросетевого преобразователя биометрия-код доступа

После обучения нейросетевого преобразователя биометрия-код доступа (однослойного или двухслойного) необходимо осуществить прогнозирование для него вероятности ошибок первого рода (ошибочного отказа пользователю «Свой» в доступе). Прогнозирование должно быть осуществлено с использованием тестовых естественных биометрических образов «Свой», не использованных ранее для обучения.

При необходимости могут быть привлечены дополнительные синтетические биометрические образы «Свой», полученные морфингом образов-родителей, либо мутациями образов-родителей по ГОСТ Р 52633.2.

9.4 Отображение результатов автоматического тестирования ошибок первого рода обученного нейросетевого преобразователя биометрия-код доступа

Интерфейс отображения результатов автоматического прогнозирования вероятности ошибок первого рода должен показывать пользователю «Свой» возможность его положительной аутентификации при нескольких последовательных попытках. Должна отображаться вероятность положительной аутентификации пользователя «Свой» при проведении им первой попытки, второй попытки и вплоть до пятой попытки аутентификации, следующих подряд.

Приложение А
(справочное)

Примеры статистик распределения входных и выходных данных нейрона первого слоя на различных этапах обучения

Входные биометрические параметры v_i, как правило, имеют распределение значений, близкое к нормальному. Примеры распределения значений биометрических параметров v_1, v_2, v_3, v_4, v_5 рукописного образа «Свой» и распределение значений тех же биометрических параметров множества случайных образов «Все «Чужие» приведены на рисунке А.1.

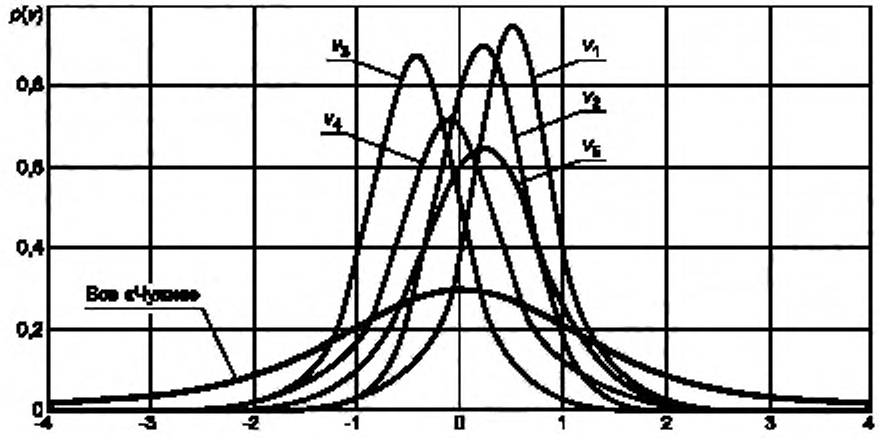

Рисунок А.1 — Примеры распределения значений биометрических параметров v_1, v_2, v_3, v_4, v_5 рукописного образа «Свой» и распределение значений тех же биометрических параметров множества случайных образов «Все «Чужие»

Из примеров на рисунке А.1 видно, что биометрические образы «Свой» имеют примерно равное число биометрических параметров с положительными и отрицательными значениями их математических ожиданий $E(v_1)$, $E(v_2)$, $E(v_3)$, $E(v_4)$, $E(v_5)$.

Для того, чтобы обучаемый нейрон на примеры образа «Свой» с высокой вероятностью давал отклик «1» [в соответствии с формулой (6)], задают знаки весовых коэффициентов обучаемого нейрона, это эквивалентно смене знака всех отрицательных математических ожиданий входных биометрических данных. Распределение значений биометрических параметров v_1, v_2, v_3, v_4, v_5 после смены знака весовых коэффициентов на фоне суммарного распределения значений биометрических образов «Все «Чужие» приведено на рисунке А.2.

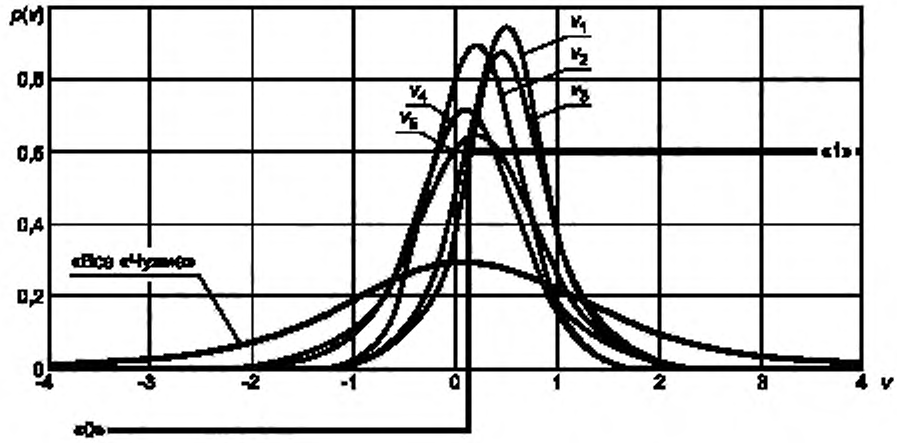

Рисунок А.2 — Распределения значений биометрических параметров v_1, v_2, v_3, v_4, v_5 после смены знака весовых коэффициентов на фоне суммарного распределения значений биометрических образов «Все «Чужие»

После вычисления весового коэффициента нейрона по формуле (5) и суммирования всех биометрических параметров нейрона происходит смещение математического ожидания отклика сумматора на примеры образа «Свой» в сторону более глубокого состояния «1» пороговой нелинейности обучаемого нейрона. Положения распределения значений откликов «Свой» на входе нелинейного элемента нейрона, соответствующие распределениям, приведенным на рисунках А.1, А.2, приведены на рисунке А.3.

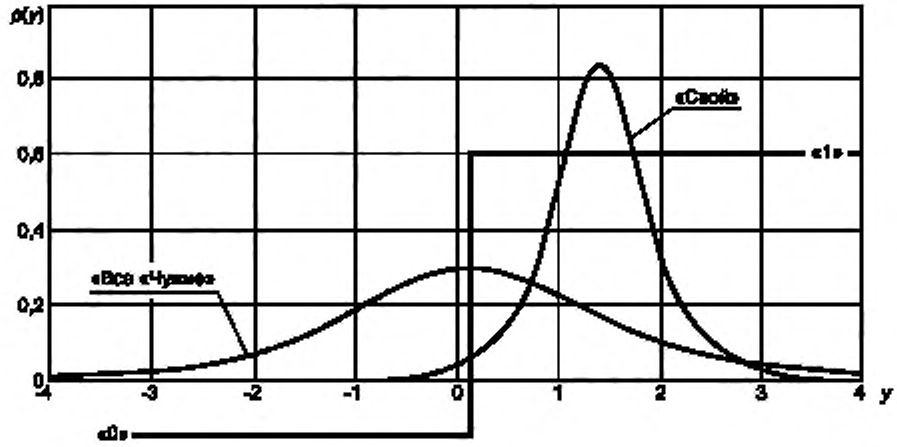

Рисунок А.3 — Распределение значений данных на выходе сумматора нейрона, обученного с вероятностью 0,95 выдавать состоянии «1» при воздействии образом «Свой» и давать равновероятные состояния «0» и «1» при воздействии случайными образами «Чужие»

УДК 681.18:006.354 ОКС 35.040

Ключевые слова: техническая защита информации, биометрия, обучение искусственных нейронов, нейронные сети, преобразователь биометрия-код доступа

Редактор *Н.В. Таланова*
Технический редактор *И.Е. Черепкова*
Корректор *И.А. Королева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 09.10.2018. Подписано в печать 24.10.2018. Формат 60×84½. Гарнитура Ариал.
Усл. печ. л. 2,33. Уч.-изд. л. 2,10.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru