УДК 519.2, 612.087, 621.319.7
DOI 10.21685/2072-3059–2017-1-4

В. И. Волчихин, А. И. Иванов, А. В. Безяев, А. В. Елфимов, А. П. Юнин

ОЦЕНКА ЭФФЕКТА УСКОРЕНИЯ ВЫЧИСЛЕНИЙ, ОБУСЛОВЛЕННОГО ПОДДЕРЖКОЙ КВАНТОВОЙ СУПЕРПОЗИЦИИ ПРИ КОРРЕКТИРОВКЕ ВЫХОДНЫХ СОСТОЯНИЙ НЕЙРОСЕТЕВОГО ПРЕОБРАЗОВАТЕЛЯ БИОМЕТРИИ В КОД

Аннотация.

Актуальность и цели. Целью работы является оценка выигрыша, возникающего из-за использования программной поддержки, эффектов квантовой суперпозиции выходных состояний нейронной сети.

Материалы и методы. Для наблюдения эффектов квантовой суперпозиции используется метод, состоящий в размывании детерминированных данных одного примера образа «Свой» данными генератора «белого шума». По этой причине часть выходных разрядов нейросетевого преобразователя оказываются нестабильными.

Результаты. Предложено использовать коды, обнаруживающие и исправляющие ошибки, хранящие синдромы связанных ошибок в виде хэш-функции от верных состояний корректируемого кода.

Выводы. Реализация самокорректирующегося кода при его длине 256 бит, способного обнаруживать и корректировать 12 ошибок, дает выигрыш в сокращении вычислений на 20 десятичных порядков. Этот выигрыш обусловлен использованием при вычислениях эффектов поддержки квантовой суперпозиции длинной 12 кубит.

Ключевые слова: квантовая суперпозиция, нейросетевой преобразователь биометрия-код, дискретный спектр выходных состояний, статистический анализ на малых выборках.

V. I. Volchikhin, A. I. Ivanov, A. V. Bezyaev, A. V. Elfimov, A. P. Yunin

EVALUATION OF THE CALCULATION ACCELERATION EFFECT, CAUSED BY THE SUPPORT OF QUANTUM SUPERPOSITION STATES DURING ADJUSTMENT OF OUTPUT CONDITIONS OF A “BIOMETRICS - CODE” NEURAL NETWORK CONVERTER

Abstract.

Background. The aim of the work is to estimate the benefit of using the program support, the effects of quantum superposition of the neural network’s output.

Materials and methods. To observe the effects of quantum superposition the authors used a method consisting in blurring of deterministic data of one “Friend” image example by "white noise" generator data. For this reason, a part of neural network convereter’s output discharges are unstable.

Results. It is proposed to use codes to detect and correct errors, storing syndromes of related errors in the form hash functions from the true state of the corrected code.

Conclusions. The implementation of the self-correcting code with its length of 256 bits, capable of detecting and correcting 12 errors, gives a benefit in reduction

of the computation by 20 orders of magnitude. This benefit is due to the use of effects of the support of quantum superposition having 12 q-bits of length.

Key words: quantum superposition, neural network “biometrics – code” converter, discrete spectrum of output states, statistical analysis on small samples.

Технология биометрической аутентификации с использованием больших искусственных нейронных сетей

В настоящее время активно идут процессы информатизации современного общества. Мы вынуждены помнить множество паролей доступа к своим личным кабинетам. При этом используемые нами пароли короткие, так как люди не способны запоминать длинные случайные цифровые последовательности. Снять проблему запоминания длинных паролей позволяют преобразователи биометрии в код. США, Канада и страны Евросоюза идут по пути использования так называемых «нечетких экстракторов» [1–3]. Россия [4] и Казахстан [5] идут по пути использования нейросетевых преобразователей биометрия-код доступа.

В силу того что информационная безопасность граждан является весьма чувствительной областью услуг, в России создан ряд стандартов, обеспечивающих возможность сертификации соответствующих аппаратно-программных продуктов. В частности, создан стандарт ГОСТ Р 52633.5 [6], регламентирующий обучение больших искусственных нейронных сетей.

Если воспользоваться стандартом ГОСТ Р 52633.5 [6], то мы получим большую сеть искусственных нейронов с большим числом входов и выходов. Пример такой сети приведен на рис. 1, где отображен один из нейронов сети с 32 входами и двумя таблицами. В левой части рисунка показана таблица связей входов *k*-го нейрона со входами нейронной сети в целом.

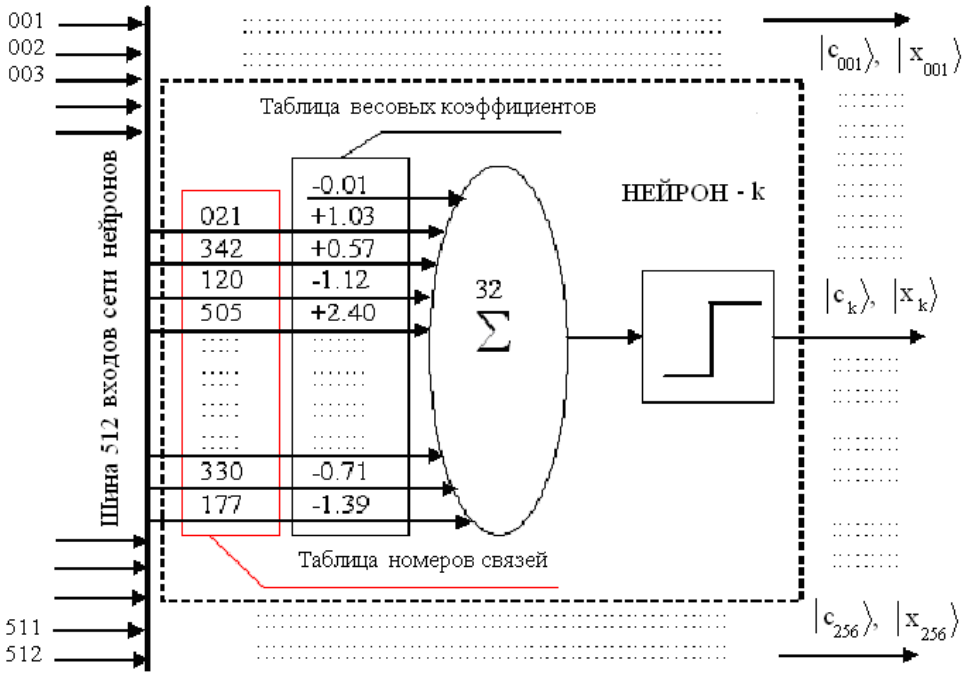

Рис. 1. Типовая схема организации нейросетевого преобразователя биометрия-код

По стандарту [6] эта таблица содержит случайные адреса, полученные от программного генератора псевдослучайных чисел. Вторая таблица содержит весовые коэффициенты нейрона, полученные в результате его обучения на нескольких примерах образа «Свой».

Следует отметить, что нейросетевой преобразователь биометрия-код ведет себя совершенно по-разному для образа «Свой» и образов «Чужие». Более того, разницу в поведении состояний нейронов удается увидеть только в том случае, если организовать условия поддержки на выходах нейронной сети квантовой суперпозиции [7]. В связи с тем, что корректно описать состояния нейронов удается только в терминах квантовых преобразований, на рис. 1 выходные состояния нейронов даны в скобках Дирака. Обозначение $|c_k\rangle$ соответствует кубиту выходного состояния k-го нейрона при воздействии на обученную сеть нейронов образом «Свой». Обозначение $|x_k\rangle$ соответствует кубиту выходных состояний k-го нейрона при воздействии на обученную нейронную сеть биометрическими образами «Чужой».

Геометрическая интерпретация работы нейросетевого преобразователя

Если считать, что континуум примеров образа «Свой» находится в некотором 512-мерном гиперэллипсе, каждый пример образа «Свой» является точкой в этом 512-мерном гиперэллипсе. Если мы возьмем любую пару контролируемых биометрических параметров, то по ним можно сделать сечение гиперэллипса. Сечение даст обычный эллипс, приведенный на рис. 2.

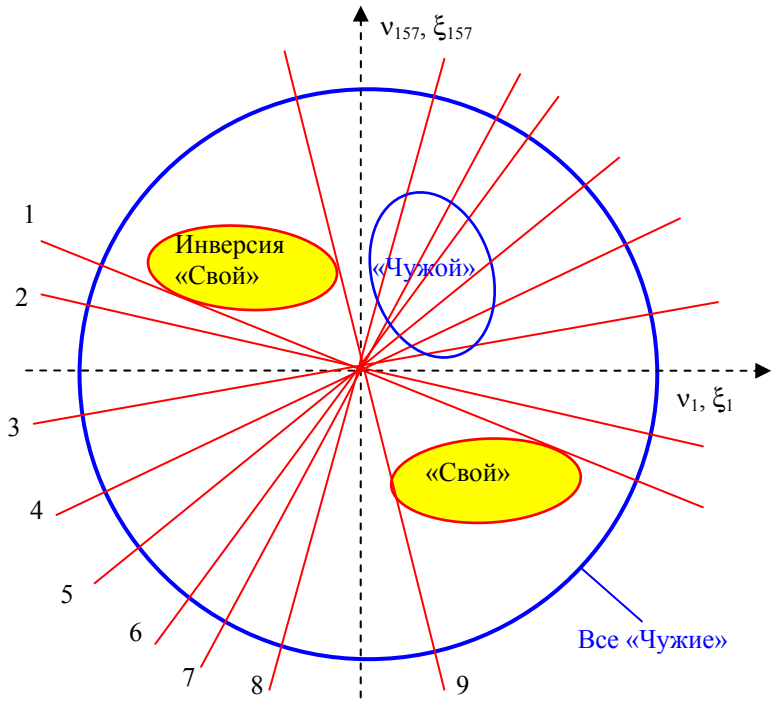

Рис. 2. Двухмерное сечение многомерной области все «Чужие»

Каждый обученный нейрон в таком сечении будет давать линию, делящую пространство все «Чужие» пополам. Алгоритм обучения ГОСТ Р 52633.5 [6] обеспечивает прохождение всех линий через центр гиперсферы все «Чужие» для того, чтобы состояния «0» и «1» на выходах нейронов были равновероятны. Второе условие, обеспечиваемое алгоритмом обучения ГОСТ Р 52633.5 [6], состоит в том, что ни одна из разделяющих линий (проекций разделяющих гиперплоскостей) не должна пересекать эллипс «Свой». Тогда любая точка в теле гиперэллипса «Свой» будет давать код "$\overline{c}$" или вектор состояний разрядов кода на выходах нейронов. Код «Свой» почти детерминирован, любой пример образа «Свой» дает заданное при обучении состояние выходов нейронов.

Если на его входы нейросети подаются данные примеров образа «Свой», то нейросетевой преобразователь свертывает все нестабильности образа в точку единственного криптографического ключа "$\overline{c}$". Энтропия исходных непрерывных данных вектора биометрических параметров $\overline{\nu}$ уменьшается практически до нуля энтропии выходного кода «Свой»:

$$H(\overline{\nu}) >> H("\overline{c}") \approx 0 . \quad (1)^1$$

Совершенно такая же ситуация возникает для инверсного образа «Свой», дающего инверсный выходной код "$\neg\overline{c}$" нейронной сети:

$$H(-\overline{\nu}) >> H("\neg\overline{c}") \approx 0 . \quad (2)$$

Совершенно иная ситуация возникает, если на вход нейронной сети подать 512-мерный вектор данных, принадлежащих биометрическому образу «Чужой» $\overline{\xi}$. Как показано на рис. 2, через тело гиперэллипса «Чужой» проходит несколько гиперплоскостей нейронов, обученных распознавать образ «Свой». То есть предъявление нейронной сети данных примеров «Чужой» приводит к изменению выходных кодов нейронной сети. Каждый пример образа «Чужой» дает свой код на выходах нейросети. Несмотря на то, что энтропия естественной нестабильности примеров образа «Свой» и примеров образов «Чужой» сопоставимы, энтропия их выходных кодов оказывается очень большой:

$$H(\overline{\nu}) \approx H(\overline{\xi}) < H("\overline{x}") >> 0 . \quad (3)$$

Получается, что обученная нейронная сеть практически полностью устраняет естественную энтропию нестабильности многомерных континуумов входных данных образа «Свой». В этом случае нейросеть выполняет функцию, обратную функции хэширования (1). Хэширование (перемешивание) – это всегда функция усиления энтропии. Для образов «Чужой» все наоборот, нейросеть осуществляет функцию хэширования биометрических данных (3). Энтропия образа «Чужой» усиливается.

[1] В уравнении (1) присутствует вектор континуумов и вектор двоичных разрядов кода. Для того чтобы их различать, вектор дискретных состояний помечен кавычками, что является общепринятой записью для языков программирования высокого уровня и принято в литературе по нейросетевой биометрии.

Переход от описания обычных бинарных биокодов в пространство расстояний Хэмминга

Отечественные нейросетевые преобразователи имеют 256 выходов [4] в силу того, что российские стандарты шифрования и формирования цифровой подписи построены на использовании криптографических ключей длиной 256 бит. Кроме того, ОС Windows и ОС Linux способны работать с паролями доступа длиной до 256 бит (32 символа в 8-битной кодировке). Обычно люди используют короткие пароли, так как не могут запоминать длинные пароли из случайных символов. Биометрия снимает проблему длинных паролей. Любой пользователь получает через биометрию возможность преобразовать свой короткий, легко запоминаемый пароль, в длинный код доступа. Когда нет проблемы запоминания длинных паролей, нет необходимости экономить на их длине. Если ОС Windows позволяет использовать пароль максимальной длины в 256 бит, то такие пароли и нужно использовать.

Описать все состояния длинных кодов технически невозможно. Одним из приемов упрощения статистического описания длинных кодов является переход в пространство расстояний Хэмминга. Далее будет показано, что этот прием сильно упрощает расчет энтропии выходных состояний нейронной сети.

Одной из самых популярных является метрика Хэмминга расстояний между кодами «Чужой» и кодом «Свой»:

$$h = \sum_{i=1}^{256} \left("c_i"\right) \oplus \left("x_i"\right), \tag{4}$$

где $"c_i"$ – один из разрядов кода «Свой»; $"x_i"$ – один из разрядов кода «Чужой»; $\oplus$ – операция сложения по модулю два.

Также используется расстояние Хэмминга между центром кодов «Чужой-*k*» и другими кодами других образов все «Чужие»:

$$h = \sum_{i=1}^{256} "E\left("x_{k,i}"\right)" \oplus \left("x_i"\right), \tag{5}$$

где $"E("x_{k,i}")"$ [1] – наиболее вероятное состояние *i*-го разряда кода «Чужой-*k*»:

$$\begin{cases} "E("x_{k,i}")" \leftarrow "0" \text{ если } P("0") > P("1"), \\ "E("x_{k,i}")" \leftarrow "1" \text{ если } P("1") > P("0"), \\ "E("x_{k,i}")" \leftarrow rnd("0","1") \text{ если } P("1") = P("0"). \end{cases} \tag{6}$$

Если вероятности состояний «0» и «1» одинаковы, то состояние $"E("x_{k,i}")"$ выбирается случайно.

Следует отметить, что записать квантовую суперпозиция для 256 кубит выходного кода нейронной сети для образа «Чужой» технически невозможно. Однако как только мы будем описывать состояния выходных разрядов в про-

[1] В записи проявились двойные кавычки, что означает действие дискретного преобразования (6) над дискретной переменной.

странстве расстояний Хэмминга (по отношению к коду «Свой» или к коду центра образа «Чужой-*k*» проблема статистического описания квантовой суперпозиции снимается. Для ее решения достаточно построить гистограмму соответствующего распределения расстояний Хэмминга. Плотности распределения значений расстояний Хэмминга $p(h)$ достаточно для симметричного статистического описания нейронной сети [4, 5] или в виде симметричной связки квантовой суперпозиции и квантовой сцепленности [7].

Квантовая суперпозиция для одиночного разряда биокода

Следует подчеркнуть, что разряды кодов примеров образа «Свой» стабильны. В левом верхнем углу на рис. 3 дана гистограмма показателей стабильности распределения разрядов кода "$\overline{c}$". Показатель стабильность разрядов кода введен ГОСТ Р 52633.3–2011 [8]:

$$\omega_i = 2 \cdot \left|1 - P("0_i")\right| = 2 \cdot \left|1 - P("1_i")\right|, \qquad (7)$$

где вероятности состояний разряда определяются при предъявлении нейронной сети примеров одного образа «Чужой».

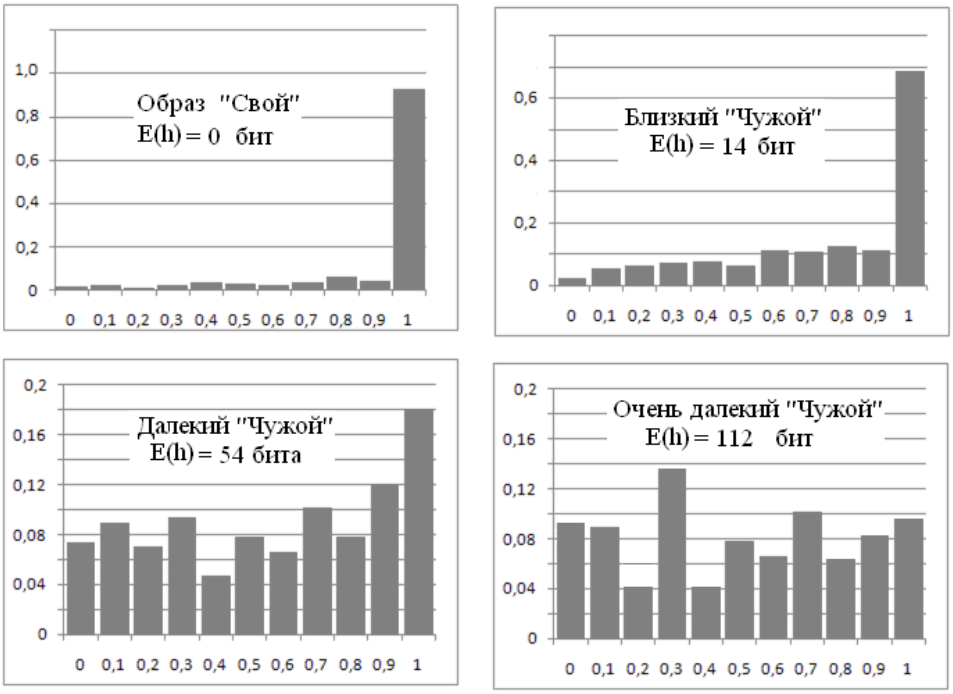

Рис. 3. Примеры гистограмм распределения показателей стабильности образов «Чужой-*k*» в зависимости от математического ожидания расстояний Хэмминга их примеров до кода образов «Свой»

Показатель стабильности игнорирует наиболее вероятное состояние *i*-го разряда кода "$E("x_{k,i}")$" и отражает только его стабильность. Если *i*-й разряд кодов абсолютно стабилен, то показатель оказывается единичным $\omega_i = 1$. Если вероятности двух состояний разряда совпадают $P("0_i") = P("1_i") = 0{,}5$, то показатель стабильности оказывается нулевым $\omega_i = 0$.

Для *i*-го разряда кода «Свой» полная квантовая суперпозиция записывается следующим образом [9]:

$$\left|\Psi_i\right\rangle = \sqrt{P("0_i")} \cdot \left|0_i\right\rangle + \sqrt{P("1_i")} \cdot \left|1_i\right\rangle . \quad (8)$$

Однако примерно 90 % разрядов кода «Свой» оказываются абсолютно стабильными, и в их вантовой суперпозиции (8) одна из компонент исчезает. То есть эти стабильные разряды оказываются полностью детерминированными и их нельзя рассматривать как кубиты. Только 10 % разрядов кода «Свой» следует рассматривать как кубиты и описывать соотношением (8).

Из данных рис. 3 видно, что удаление центра кодов образа «Чужой-*k*» от кода «Свой» приводит к росту математического ожидания расстояний Хэмминга:

$$E(h) \approx \sum_{i=1}^{256} (1-\omega_i) \cdot "E\left("x_{k,i}"\right)"\oplus\left("c_i"\right). \quad (9)$$

Чем выше расстояние Хэмминга между центром образа «Чужой-*k*» и кодом «Свой», тем менее стабильными оказываются разряды кода. Самыми нестабильными разрядами обладают коды, имеющие центр расстояний Хэмминга, равный половине длин кодов.

Если расстояние до центра кодов больше половины, то необходимо переходить к определению расстояний Хэмминга до инверсного кода «Свой»:

$$E(\neg h) \approx \sum_{i=1}^{256} (1-\omega_i) \cdot "E\left("x_{k,i}"\right)"\oplus\left("\neg c_i"\right). \quad (10)$$

Самые нестабильные коды имеют примерно 10 % почти стабильных разрядов (нижний правый угол рис. 3) и примерно равномерную гистограмму распределения показателей стабильности во всем диапазоне ее значений.

Поддержка квантовой суперпозиции на выходах обученной нейронной сети при коррекции ошибок кода «Свой»

Самым простым техническим применением квантовой суперпозиции кодов на выходах нейронной сети является исправление ошибок кода «Свой». Следует отметить, что классические коды корректировки ошибок используются «нечеткими экстракторами» [1–3]. Исследование «нечетких экстракторов» [10] показало, что они по всем параметрам хуже нейросетевых преобразователей биометрия-код. Структурные схемы преобразователей биометрия-код и «нечетких экстракторов» приведены на рис. 4.

«Нечеткие экстракторы» отображены в левой части рис. 4. Они построены на том, что «сырые» контролируемые биометрические параметры квантуются. При этом длинный код имеет до 30 % ошибок. Поправить 30 % ошибок существующими самокорректирующимися кодами нельзя [11].

Например, коды БЧХ (Боуза – Чоудхуры – Хоквинчхема) длиной 512 бит способны поправить не более 11 % ошибок, как это показано на рис. 5.

Практика применения БЧХ-кодов в «нечетких экстракторах» обычно строится на применении 20-кратной избыточности (2000 % на шкале рис. 5)

и маскировании части наиболее нестабильных разрядов. В итоге скорректированный код будет иметь всего 25 разрядов. По этой причине выходные коды «нечетких экстракторов» короткие (рис. 4).

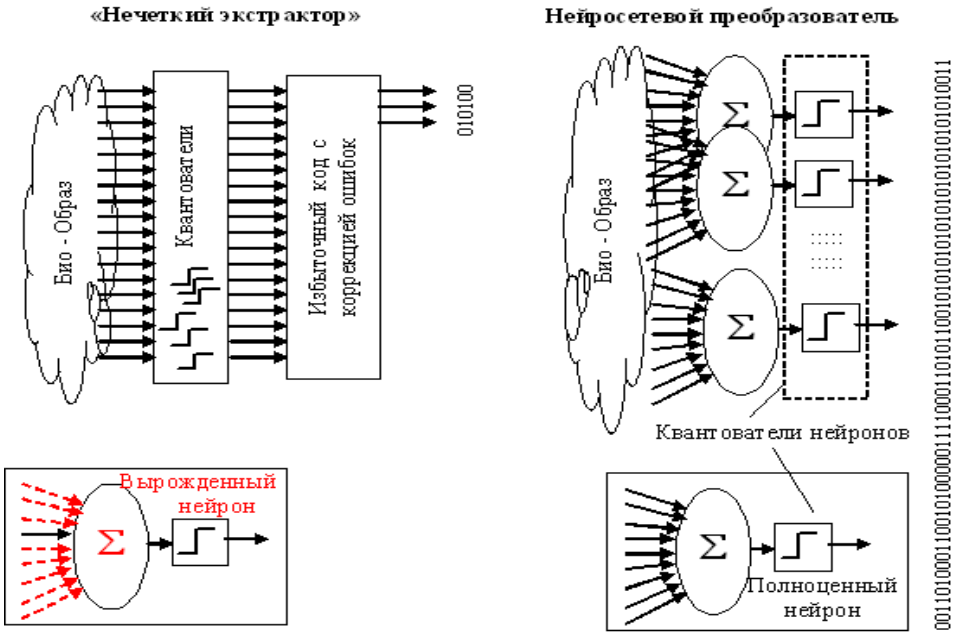

Рис. 4. Блок-схемы организации «нечетких экстракторов»
и нейросетевых преобразователей биометрия-код

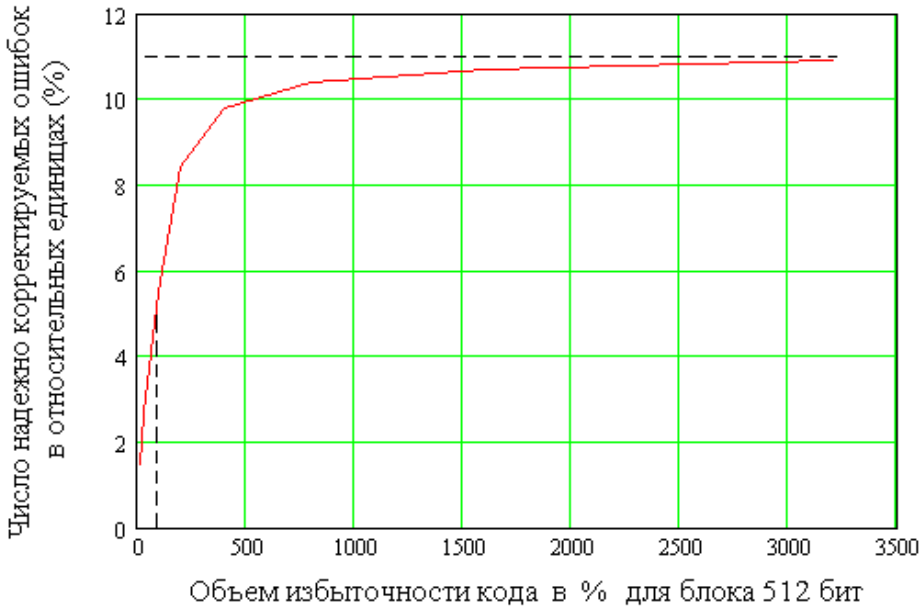

Рис. 5. Связь размеров избыточности кода БЧХ
с его корректирующей способностью

Нейросетевые преобразователи биометрия-код работают иначе, чем «нечеткие экстракторы». Нейроны имеют входные сумматоры, на которых строятся линейные функционалы обогащения данных. Уже обогащенные данные на выходе сумматора квантуются. В итоге выходной код нейросетевых преобразователей оказывается длинным, примерно в 10 раз длиннее выходных кодов «нечетких экстракторов». При этом выходные коды оказываются стабильными с вероятностью 0,9. А с вероятностью 0,1 возникают одиночные ошибки в 1, 2 разрядах.

В наихудшем случае грубой ошибки биометрических данных на выходах нейронной сети могут появиться от 10 до 20 ошибок. Покажем, что вычисления, осуществляемые при корректировке ошибок кода «Свой», многократно упрощаются, если создать условия наблюдения квантовой суперпозиции разрядов кода.

Во время работы нейросетевого преобразователя в режиме аутентификации нет возможности применения нескольких примеров проверяемого образа. В связи с этим необходимо их создать. Это может быть сделано путем добавления к единственному примеру размывающего данные шумом. Схема численных преобразований приведена на рис. 6. Практика показывает, что для наблюдения квантовой суперпозиции необходимо использовать программный генератор псевдослучайных данных с амплитудой шума $0{,}1\cdot\sigma(\nu)$.

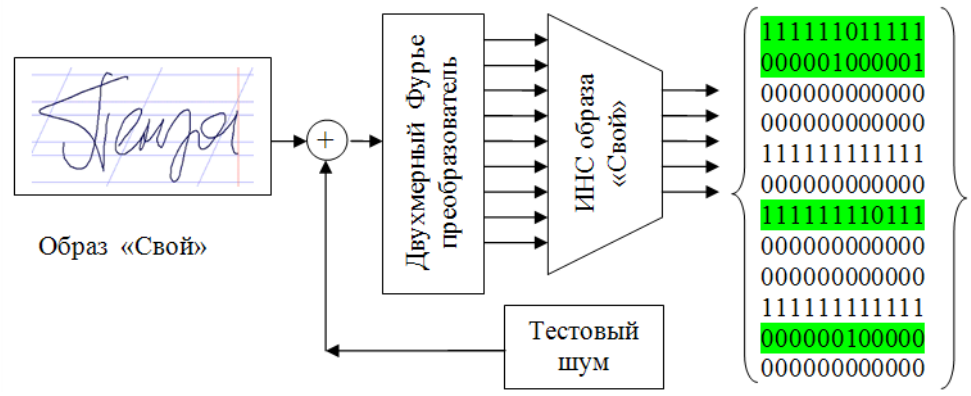

Рис. 6. Отклик обученной нейронной сети
на известный ей образ «Свой», размытый тестовым шумом

Код части разрядов на выходе нейронной сети оказывается нестабильным, на рис. 6 эти разряды выделены заливкой. Корректирующие коды [12, 13] строятся на связывании всех разрядов кода криптографическим хэшированием:

$$"\overline{xx}" = \text{hash}("\overline{c}")\,. \qquad (11)$$

Функция хэширования вычисляется в момент обучения нейронной сети, когда код "$\overline{c}$" известен. Эталонное значение хэш-функции "$\overline{xx}$" запоминают и безопасно хранят в контейнере нейронной сети. Безопасность хранения данных после их хэширования обусловлена необратимостью криптографических хэш-функций. Применение хэширования как связывающей функции позволяет легко обнаруживать все ошибки кода. Изменение даже одного

бита в коде приводит к изменению примерно половины состояний разрядов хэш-функции.

Предположим, что мы при зашумлении проверяемых данных обнаружили 12 нестабильных бит. Пользуясь этим, мы должны проверить все возможные состояния 12 нестабильных бит и для каждого вычислить хэш-функцию от полного числа со стабильными битами и нестабильными битами. Всего придется проверить $12! = 4790016$ состояний. Программные реализации криптографических хэш-функций оптимизированы и быстро вычисляются. Для проверки 12! состояний на обычном компьютере сегодня потребуется порядка 10 с (без аппаратных ускорителей вычислений нужной хэш-функции).

Если бы мы перебирали все 256 состояний, то нам потребовалось бы проверить $\prod_{i=0}^{12}(256-i)$ состояний. То есть для рассматриваемого нами случая мы имеем огромное сокращение объема вычислений при корректировке ошибок:

$$\frac{\prod_{i=0}^{12}(256-i)}{12!} \approx 10^{21}. \qquad (12)$$

Таким образом, использование поддержки квантовой суперпозиции при корректировании кодов позволяет снизить вычислительную сложность задачи на 20 порядков. Нейросеть с хэш-корректором ошибок позволяет исправлять практически все ошибки биометрического образа «Свой». То есть вместо 11 % ошибок, исправляемых БЧХ-кодом «нечетких экстракторов», мы получаем код, способный корректировать от 30 до 50 % ошибок в «сырых» данных. Все это следствие замены «нечетких экстракторов» более сложными искусственными нейронными сетями и применение поддержки на их выходах квантовой суперпозиции длинной в 12 кубит. Все другие – стабильные биты нейронной сети – нет смысла рассматривать через их описание квантовой суперпозицией. При корректировке ошибок и проверке всех возможных состояний кода нас интересуют только нестабильные биты, и только к ним применимы вычислительные приемы квантовой математики. То что мы, поддерживая 12-кубитную квантовую суперпозицию нестабильных разрядов кода, сокращаем вычислительные затраты на 20 порядков, является ярким примером ускорения вычислений через использование квантовых преобразований.

Если отказаться от поддержки квантовой суперпозиции в 12 кубит, то вместо 10 с корректировки кода с 12 ошибками придется ждать более миллиарда лет.

Заключение

Выигрыш от использования квантовых вычислителей не зависит от того, на какой элементной базе они реализованы. Достижимое ускорение квантовых вычислений в первую очередь зависит от длины квантовой суперпозиции, которую может поддерживать вычислитель. Быстродействие используемых вычислительных элементов играет второстепенную роль. Так как ускорение вычислений является экспонентой, достаточно незначительного увеличения длины квантовой суперпозиции для того, чтобы покрыть задержки вычислений, связанные с использованием старой элементной базы. Нет необходимо-

сти создавать новую элементную базу вычислительной техники, ориентированную только под квантовые вычисления в рамках парадигмы Манина – Шредингера [9]. Как показано в данной статье, квантовую суперпозицию без особых проблем можно поддерживать на выходах искусственной нейронной сети, воспроизводимой на обычном компьютере. Поддержка квантовой суперпозиции даже для 12 кубит уже способна давать огромный выигрыш вычислительных затрат обычной вычислительной машины, воспроизводящей вычисления.

Библиографический список

1. **Dodis, Y.** Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy / Y. Dodis, L. Reyzin, A. Smith // Proc. EUROCRYPT. – 2004. – April 13. – P. 523–540.
2. **Monrose, F.** Cryptographic key generation from voice / F. Monrose, M. Reiter, Q. Li, S. Wetzel // Proc. IEEE Symp. on Security and Privacy. – 2001. – P. 202–213.
3. **Ramírez-Ruiz, J.** Cryptographic Keys Generation Using FingerCodes / J. Ramírez-Ruiz, C. Pfeiffer, J. Nolazco-Flores // Advances in Artificial Intelligence – IBERAMIA-SBIA 2006 (LNCS 4140). – 2006. – P. 178–187/
4. Нейросетевая защита персональных биометрических данных / Ю. К. Язов, В. И. Волчихин, А. И. Иванов, В. А. Фунтиков, И. Г. Назаров ; под ред. Ю. К. Язова. – М. : Радиотехника, 2012. – 157 с.
5. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа : моногр. / Б. С. Ахметов, А. И. Иванов, В. А. Фунтиков, А. В. Безяев, А. Ю. Малыгин. – Казахстан, Алматы : Изд-во LEM, 2014. – 144 с. – URL: http://portal.kaznu.kz/files/publicate/2014-06-27-11940.pdf
6. ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа. – М., 2011.
7. **Иванов, А. И.** Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции / А. И. Иванов. – Пенза : Изд-во АО «ПНИЭИ», 2016.– 133 с. – URL: http://пниэи.рф/activity/science/BOOK16.pdf
8. ГОСТ Р 52633.3–2011. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора. – М., 2011.
9. **Нильсон, М.** Квантовые вычисления и квантовая информация / М. Нильсон, И. Чанг. – М. : Мир. 2006. – 821 с.
10. **Иванов, А. И.** Нечеткие экстракторы: проблема использования в биометрии и криптографии / А. И. Иванов // Первая миля. – 2015. – № 1. – С. 40–47.
11. **Морелос-Сарагоса, Р.** Искусство помехоустойчивого кодирования / Р. Морелос-Сарагоса. – М. : Техносфера, 2007. – 320 с.
12. **Безяев, А. В.** Нейросетевой преобразователь в самокорректирующийся код, совершенно не обладающий избыточностью / А. В. Безяев // Нейрокомпьютеры: разработка, применение. – 2012. – № 3. – С. 52–55.
13. **Безяев, А. В.** Оптимизация структуры самокорректирующегося биокода, хранящего синдромы ошибок в виде фрагментов хеш-функций / А. В. Безяев, А. И. Иванов, В. А. Фунтиков // Вестник Уральского федерального округа. Безопасность в информационной сфере. – 2014. – № 3 (13). – С. 4–14.

References

1. Dodis Y., Reyzin L., Smith A. *Proc. EUROCRYPT*. 2004, April 13, pp. 523–540.
2. Monrose F., Reiter M., Li Q., Wetzel S. *Proc. IEEE Symp. on Security and Privacy*. 2001, pp. 202–213.

3. Ramírez-Ruiz J., Pfeiffer C., Nolazco-Flores J. *Advances in Artificial Intelligence – IBERAMIA-SBIA 2006 (LNCS 4140)*. 2006, pp. 178–187/
4. Yazov Yu. K., Volchikhin V. I., Ivanov A. I., Funtikov V. A., Nazarov I. G. *Neyrosetevaya zashchita personal'nykh biometricheskikh dannykh* [Neural network protection of personal biometric data]. Moscow: Radiotekhnika, 2012, 157 p.
5. Akhmetov B. S., Ivanov A. I., Funtikov V. A., Bezyaev A. V., Malygin A. Yu. *Tekhnologiya ispol'zovaniya bol'shikh neyronnykh setey dlya preobrazovaniya nechetkikh biometricheskikh dannykh v kod klyucha dostupa: monogr.* [A technique of using large neural networks for conversion of fuzzy biometric data into access key code: monograph]. Kazakhstan, Almaty: Izd-vo LEM, 2014, 144 p. Available at: http://portal.kazntu.kz/files/publicate/2014-06-27-11940.pdf
6. GOST R 52633.5–2011. *Zashchita informatsii. Tekhnika zashchity informatsii. Avtomaticheskoe obuchenie neyrosetevykh preobrazovateley biometriya-kod dostupa* [Data protection. Information protecting technology. Autmatic learning of neural network "biometrics - code" converters]. Moscow, 2011.
7. Ivanov A. I. *Mnogomernaya neyrosetevaya obrabotka biometricheskikh dannykh s programmnym vosproizvedeniem effektov kvantovoy superpozitsii* [Multidimensional neural network processing of biometric data with program reproduction of quantum superposition effects]. Penza: Izd-vo AO «PNIEI», 2016, 133 p. Available at: http://pniei.pf/activity/science/BOOK16.pdf
8. GOST R 52633.3–2011. *Zashchita informatsii. Tekhnika zashchity informatsii. Testirovanie stoykosti sredstv vysokonadezhnoy biometricheskoy zashchity k atakam podbora* [Data protection. Information protecting technology. Testing of high-reliability biometric protection device resistance to key searching attacks]. Moscow, 2011.
9. Nil'son M., Chang I. *Kvantovye vychisleniya i kvantovaya informatsiya* [Quantum calculations and quantum informatics]. Moscow: Mir, 2006, 821 p.
10. Ivanov A. I. *Pervaya milya* [The first mile]. 2015, no. 1, pp. 40–47.
11. Morelos-Saragosa R. *Iskusstvo pomekhoustoychivogo kodirovaniya* [The art of noise-immune coding]. Moscow: Tekhnosfera, 2007, 320 p.
12. Bezyaev A. V. *Neyrokomp'yutery: razrabotka, primenenie* [Neurocomputers: development, aplication]. 2012, no. 3, pp. 52–55.
13. Bezyaev A. V., Ivanov A. I., Funtikov V. A. *Vestnik Ural'skogo federal'nogo okruga. Bezopasnost' v informatsionnoy sfere* [Bulletin of Ural Federal District. Information field security]. 2014, no. 3 (13), pp. 4–14.

Волчихин Владимир Иванович
доктор технических наук, профессор, президент Пензенского государственного университета (Россия, г. Пенза, ул. Красная, 40)

E-mail: president@pnzgu.ru

Volchikhin Vladimir Ivanovich
Doctor of engineering sciences, professor, President of Penza State University (40 Krasnaya street, Penza, Russia)

Иванов Александр Иванович
доктор технических наук, доцент, начальник лаборатории биометрических и нейросетевых технологий, Пензенский научно-исследовательский электротехнический институт (Россия, г. Пенза, ул. Советская, 9)

E-mail: ivan@pniei.penza.ru

Ivanov Aleksandr Ivanovich
Doctor of engineering sciences, associate professor, head of the laboratory of biometric and neural network technologies, Penza Research Institute of Electrical Engineering (9 Sovetskaya street, Penza, Russia)

Безяев Александр Викторович
кандидат технических наук, ведущий специалист, Пензенский филиал Научно-технический центр «Атлас» (Россия, г. Пенза, ул. Советская, 9)

E-mail: Bezyaev_Alex@mail.ru

Bezyaev Aleksandr Viktorovich
Candidate of engineering sciences, leading specialist of STC "Atlas" branch in Penza (9 Sovetskaya street, Penza, Russia)

Елфимов Андрей Владимирович
инженер, Филиал «Аргус» Пензенского научно-исследовательского электротехнического института (Россия, г. Пенза, пр. Победы, 69,а)

E-mail: drec@yandex.ru

Elfimov Andrey Vladimirovich
Engineer, "Argus" branch of Penza Research Electrotechnical Institute (69a Pobedi avenue, Penza, Russia)

Юнин Алексей Петрович
начальник научно-исследовательского отдела, Пензенский научно-исследовательский электротехнический институт (Россия, г. Пенза, ул. Советская, 9)

E-mail: ivan@pniei.penza.ru

Yunin Aleksey Petrovich
Head of research department, Penza Research Institute of Electrical Engineering (9 Sovetskaya street, Penza, Russia)

УДК 519.2, 612.087, 621.319.7

Оценка эффекта ускорения вычислений, обусловленного поддержкой квантовой суперпозиции при корректировке выходных состояний нейросетевого преобразователя биометрии в код / В. И. Волчихин, А. И. Иванов, А. В. Безяев, А. В. Елфимов, А. П. Юнин // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2017. – № 1 (41). – С. 43–55. DOI 10.21685/2072-3059–2017-1-4