Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 9, Пенза-2014, с. 12-13 (http://www.pniei.penza.ru/RV-conf/T9/C12)

УСЛОВИЕ КОРРЕКТНОЙ ОЦЕНКИ СТОЙКОСТИ К АТАКАМ ПОДБОРА ПРЕОБРАЗОВАТЕЛЕЙ БИОМЕТРИЯ-КОД С НЕЙРОНАМИ, ОСУЩЕСТВЛЯЮЩИМИ МНОГОУРОВНЕВОЕ КВАНТОВАНИЕ

Малыгина Е.А. (Пенза)

Появление атаки Маршалко [1] на нейросетевые преобразователи биометрия-код заставляет взглянуть по новому на проблему выбора выходных квантователей у нейронов. На сегодняшний день в нейронах обычно используют двоичные выходные квантователи (левая часть рис. 1), однако можно усложнить процедуру квантования и использовать, например, трех уровневые выходные квантователи (правая часть рис. 1).

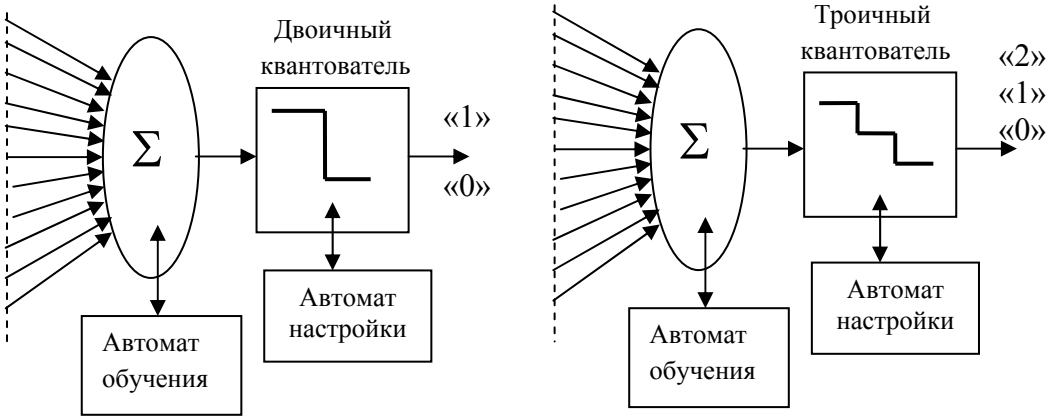

Рис. 1. Пример двоичного нейрона (левая часть рисунка) и троичного нейрона (правая часть рисунка)

Очевидно, что переход от двоичных квантователей к более сложным квантователям с большим числом выходных состояний дает возможность получать на выходе нейрона больше информации о образе «Свой» и образе «Чужой». В частности переход от применения двоичных нейронов к троичным нейронам в первом приближении должен увеличивать эффективную длину выходного биометрического ключа в полтора раза.

Естественно, что при переходе к троичным нейронам уже нельзя будет пользоваться алгоритмом их обучения по ГОСТ Р 52633.5-2012. Необходимо будет разрабатывать новый стандарт по автоматическому обучению нейронных сетей, состоящих из нейронов с Т-арными (троичными, четырехичными, пятиричными,…) квантователями. Предположительно, что новый стандарт должен будет строиться на разделении между собой автоматов обучения весовых коэффициентов сумматоров нейронов и автоматов настройки (Т-1) порогов Т-арных квантователей.

Необходимость разделения процедур «обучения сумматора» и «настройки нелинейности» связана с тем, что только в этом случае [2, 3] удается сделать эти процедуры быстрыми и устойчивыми. Задача идентификации нелинейных объектов [2] и задача обучения нейронных сетей [3] являются топологическими близнецами. И в том и в другом случае раздельное описание нелинейных

свойств объекта и линейных сверток данных является конструктивной формализацией.

Еще одним важным моментом является то, что при переходе к использованию Т-арных нейронов энтропию выходных состояний нейросети удается увеличить более чем в Т/2 раз, если отказаться от применения только «монотонных квантователей», показанных на рисунке 1. Если перейти к применению «немонотонных квантователей» (рис. 2) число возможных состояний нейросетевого преобразователя значительно увеличивается.

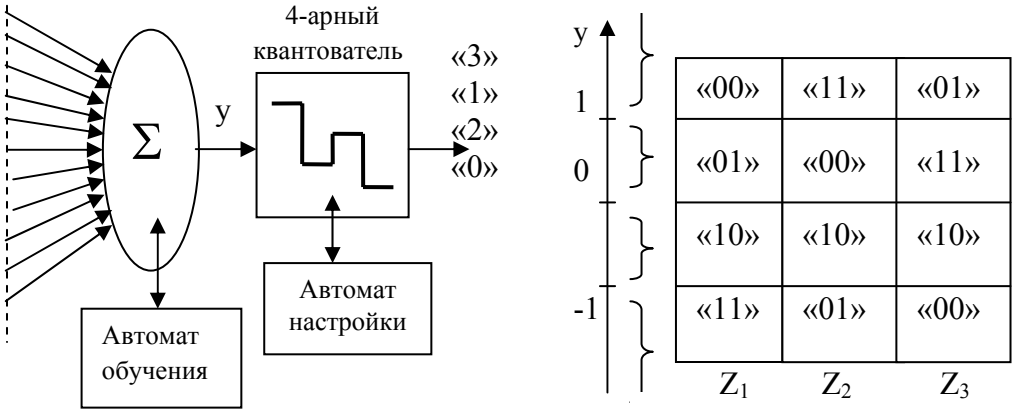

Рис. 2 Четырех-арный нейрон, квантователь которого может иметь 4! вариантов форм, описываемых тремя порогами и 25 таблицами возможных состояний

Увеличение энтропии более чем в Т/2 раз связано с тем, что не монотонные квантователи имеют большое (Т!) число возможных форм. Например эти формы могут быть заданы порогами переключения и таблицами состояний (правая часть рисунка 2). Использование не монотонных нелинейностей фактически эквивалентно применению некоторых табличных не криптографических функций хэширования, повышающих энтропию выходных состояний нейросетевого преобразователя биометрия-код.

ГОСТ Р 52633.3-2011 прямо указывает на то, что при оценке стойкости к атакам подбора механизмы размножения биометрических ошибок должны быть отключены. То есть при тестировании стойкости Т-арного нейросетевого преобразователя биометрия-код недопустимо использование табличного хэширования, перед тестирование все внутренние таблицы Т-арных квантователей должны быть заменены одной монотонной таблицей (например, таблицей Z_1 монотонно убывающих кодовых состояний «11», «10», «01», «00»).

Литература:

1. Маршалко Г.Б. «Вопросы оценки стойкости нейросетевой системы биометрической аутентификации», материалы конференции «РусКрипто-2013» - http://www.ruscrypto.ru/netcat_files/File/ruscrypto.2013.051.zip
2. Иванов А.И. «Метод измерения параметров нелинейных объектов, ориентированный на применение в измерительно-вычислительных комплексах». //Автореферат на соискание ученой степени канд. техн. наук. Ленинградский электротехнический институт (ЛЭТИ) им. В.И. Ульянова (Ленина), Ленинград-1983 - 15 с.
3. Иванов А.И. Нейросетевые технологии биометрической аутентификации пользователей открытых систем. //Автореферат диссертации на соискание ученой степени докт. техн. наук по специальности 05.13.01 «Пензенский государственный университет», Пенза 2002 - 34 с.

Материал поступил 20.06.2013 г., публикуется по положительной рецензии к.т.н. Безяева А.В.