Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 8, Пенза-2012, С 36-37 (http://пниэи.рф/activity/science/BIT/T8-p36.pdf)

КОМПЛЕКСНЫЙ ПОКАЗАТЕЛЬ КАЧЕСТВА СРЕДСТВ НЕЙРОСЕТЕВОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Секретов М.В. (г. Пенза)

Оценка качества работы искусственной нейронной сети необходима для определения надежности средств высоконадежной биометрической аутентификации в целом и подтверждается результатами ее тестирования, которое проводится с использованием баз биометрических образов «Свой» и «Чужой». Тестирование искусственной нейронной сети заключается в расчете ее стойкости к атакам подбора, то есть количества попыток необходимых злоумышленнику для получения кода доступа "Свой". А также в способности искусственной нейронной сети корректно воспроизводить код доступа "Свой", определяемой допустимой вероятностью ошибки первого рода. Стандарт ГОСТ Р 52633.3 [1] устанавливает требования по оценке стойкости средств высоконадежной нейросетевой аутентификации, использующих большие и сверхбольшие искусственные нейронные сети.

Задача оценки качества работы искусственной нейронной сети требует формирования очень больших баз тестовых биометрических образов. Размеры базы должны быть достаточными для подтверждения характеристик тестируемых средств. Увеличить размеры тестовой базы биометрических образов можно за счет синтетических биометрических образов, созданных согласно стандарту ГОСТ Р 52633.2 [2]. Однако стандарт ГОСТ Р 52633.3 позволяет оценить качество работы искусственной нейронной сети с использованием малых тестовых баз содержащих около 128 примеров случайно выбранных естественных биометрических образов "Чужой".

При тестировании искусственной нейронной сети биометрические образы малой тестовой базы подаются на ее входы однократно и в произвольном порядке. Блок-схема тестирования приведена на рисунке 1.

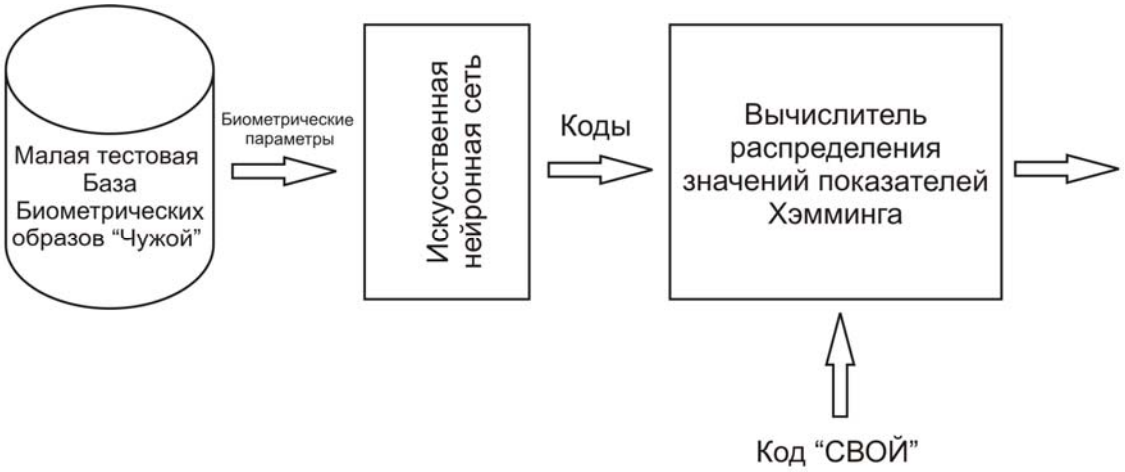

Рисунок 1 – Блок-схема тестирования искусственной нейронной сети

В процессе тестирования кодовые отклики искусственной нейронной сети сравниваются с кодом «Свой» разрядностью n, и строится распределение значений показателей критерия Хэмминга - P(h). Для численной оценки стойкости системы биометрической аутентификации к атакам подбора с разрядностью выходного кода более 32 в стандарте ГОСТ Р 52633.3 предложено использовать функцию нормального закона распределения:

$$P_2 \approx \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \cdot \int_0^{E(h)/\sigma(h)} \exp(-t^2/2)dt, \qquad (1)$$

где $E(h)$ – математическое ожидание распределения значений показателей критерия Хэмминга. $\sigma(h)$ – среднеквадратическое отклонение распределения значений показателей критерия Хэмминга.

Вероятность ошибки первого рода P_1 определяется при подаче на вход искусственной нейронной сети малой тестовой базы, включающей различные и естественные примеры биометрического образа "Свой", не участвующие в процессе обучения сети. Размер такой базы может составлять 20 примеров. Кодовые отклики искусственной нейронной сети сравниваются с кодом «Свой», которые должны быть идентичны. Примеры биометрического образа "Свой", имеющие ошибочный кодовый отклик и определяют ошибку первого рода P_1.

Показатели P_1 и P_2 позволяют оценить качество работы искусственной нейронной сети, но необходим общий комплексный показатель. Выведем зависимость общего комплексного показатель качества от вероятности ошибки первого рода и вероятности ошибки второго рода:

$$Q_{ИНС} = \frac{1}{\sqrt{P_1 \cdot P_2}} \qquad (2).$$

Таким образом, качество работы искусственной нейронной сети определяется как обратное значение среднего геометрического вероятности ошибки первого рода и вероятности ошибки второго рода. Полученный показатель качества работы искусственной нейронной сети необходим для оценки качества и надежности систем высоконадежной биометрической аутентификации и может быть применен в средствах их тестирования.

Ранее приходилось рассматривать ошибки второго рода как основной показатель взаимного сравнения средств биометрической аутентификации [3]. При этом значения ошибок первого рода не учитывались. Применение показателя (2) позволяет одновременно учитывать и вероятность ошибок первого рода и вероятность ошибок второго рода, что делает сравнение более корректным.

Литература:

1. ГОСТ Р 52633.3. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора.
2. ГОСТ Р 52633.2. Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации.
3. 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.

Материалы поступили 12.02.2012. Опубликовано 21.04.2012, рецензент д.т.н. Иванов А.И.