Труды научно-технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Том 8, Пенза-2012, с. 8-9 (http://пниэи.рф/activity/science/BIT/T8-p8.pdf)

СИНТЕЗ ФУНКЦИИ ДЛЯ ВЫЧИСЛЕНИЯ ВЕРОЯТНОСТИ ПРОПУСКА «ЧУЖОГО» ПО СТАТИСТИЧЕСКИМ ПАРАМЕТРАМ ЗАВИСИМЫХ КОДОВ-ОТКЛИКОВ «ЧУЖОЙ»

Надеев Д.Н. (г. Пенза)

В соответствии с отечественным стандартом ГОСТ Р 52633.0-2006 средства высоконадежной биометрической аутентификации рекомендуется строить на основе нейросетевых преобразователей биометрия-код. Такие преобразователи необходимо тестировать по ГОСТ Р 52633.3-2011. В соответствии с этим стандартом необходимо подавать на входы обученного преобразователя образы "Все Чужие" и получать выходные коды-отклики. По распределению выходных кодов-откликов вычисляются математическое ожидание и стандартное отклонение меры Хэмминга кодов «Чужой» и кодов «Свой». Далее по этим параметрам оценивается вероятность ложной аутентификации «Чужого». Стандартный способ вычисления вероятности пропуска «Чужого» ограничен гипотезой нормального закона распределения меры Хэмминга кодов «Чужой» не дает перспективы использования отличных от нормального законов распределения.

Еще одним способом вычисления вероятности пропуска «Чужого» является использование модификации классической схемы Бернулли с зависимыми опытами. При таком способе удается избежать ограничения связанные с гипотезой нормального закона. Текст SMathStudio-программы по аппроксимации биномиального зависимого закона распределения значений расстояний Хэмминга дан на рисунке 1.

$$n := 256 \qquad p := 0,5 \qquad r := 0,15$$

if $p < 0,4$

$$a := \left(r^2 - 9,41 \cdot r\right) \cdot (r \le 0,075) + \left(r^2 - 2,9 \cdot r - 0,49\right) \cdot (r > 0,705)$$
$$b := \left(r^2 - 4,82 \cdot r + 1\right) \cdot (r \le 0,075) + \left(r^2 - 1,432 \cdot r + 0,492\right) \cdot (r > 0,075)$$
$$c := \left(r^2 - 11,81 \cdot r + 1\right) \cdot (r \le 0,075) + \left(r^2 - 1,352 \cdot r + 0,22\right) \cdot (r > 0,075)$$

else

$$a := \left(r^2 - 5,02 \cdot r\right) \cdot (r \le 0,15) + \left(r^2 - 1,485 \cdot r - 0,53\right) \cdot (r > 0,15)$$
$$b := \left(r^2 - 4,82 \cdot r + 1\right) \cdot (r \le 0,15) + \left(r^2 - 1,432 \cdot r + 0,492\right) \cdot (r > 0,15)$$
$$c := 1$$

for $x := 0 ; x \le n ; x := x + 1$

$$t := \frac{n!}{(x!) \cdot ((n-x)!)}$$
$$f_{x+1} := t^{a+1} \cdot p^{x \cdot b} \cdot (1-p)^{(n-x) \cdot b} \cdot c$$

Рис.1. Текст программы аппроксимации биномиального зависимого закона распределения для некоммерческой среды моделирования SMath Studio

В программе задается вероятность «p» появления состояния «0» в бите кода как математическое ожидание распределения меры Хэмминга кодов «Чужой». Вторым параметром является модуль математического ожидания корреляций разрядов выходного кода [1, 2] «r». Программа выдает массив гистограммы значений плотности распределения меры Хэмминга кодов «Чужой». Первое значение выходного массива дает значение вероятности ложной аутентификации «Чужого». При вероятности p=0.5 программу можно использовать в интервале значений корреляции 0<r<0.37. При вероятности p=0.25 интервал по корреляции уменьшается в два раза до 0<r<0.18. Длина выходного кода n может меняться в интервале 32<n<512. Вероятность p может меняться в интервале 0.25<p<0.5. Результаты работы программы по вычислению плотностей распределения значений при p=0.25 и p=0.5 показаны на рисунке 2.

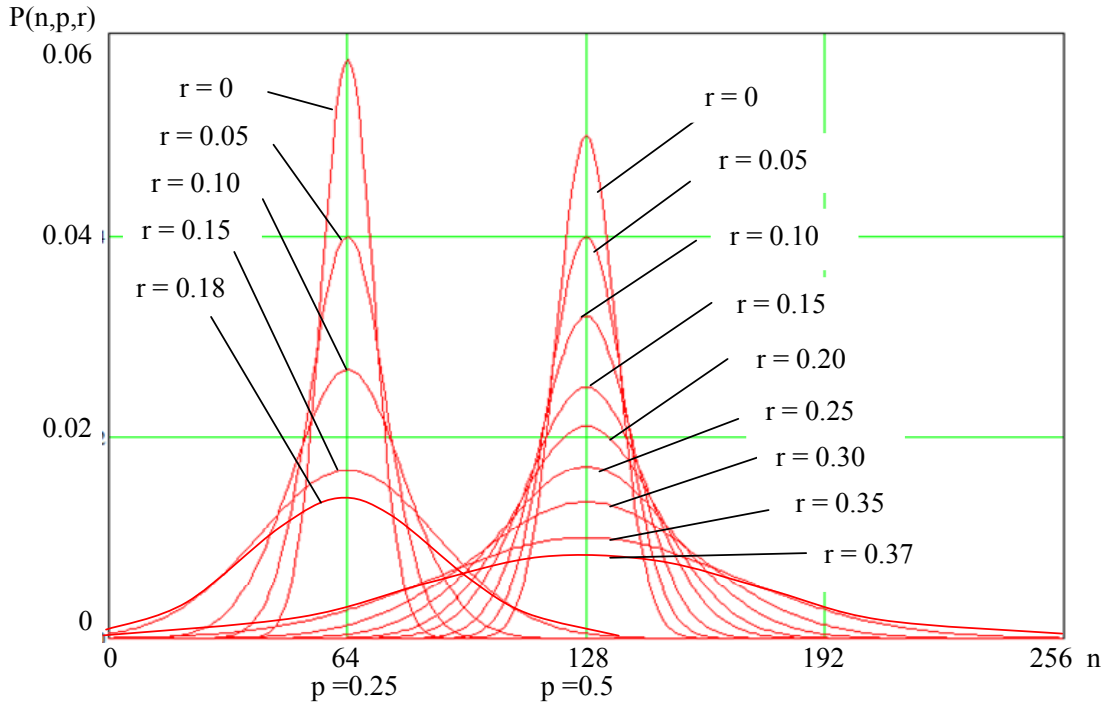

Рис. 2. Результаты работы программы при значениях p=0.25 и p=0.5.

Интервал по корреляции сжимается в два раза при уменьшении вероятности «p» в два раза. Распределения на рисунке 2 остаются нормальными при корреляции 0<r<0.37 [1, 2, 3]. При r>0.37 необходимо вместо модификации схемы Бернулли первого рода использовать модификацию второго рода [2, 3].

Таким образом, приведенная программа позволяет избежать ограничений на статистические параметры накладываемые гипотезой нормальности, использованной в ГОСТ Р 52633.3-2011.

Литература:

1. Надеев Д.Н. Табличное описание несимметричных распределений меры Хэмминга выходного кода нейросетевого преобразователя биометрия-код / «Нейрокомпьютеры, разработка, применение» № 12 2011 г, с. 8-10.

2. Надеев Д.Н. Моделирование распределения меры Хэмминга выходного кода нейросетевого преобразователя биометрия-код / «Защита информации» № 10 2010 г, с. 13-16.

3. http://86ex1h6rqbzd1d6n.p2012enza.narod2.ru

Материалы поступили 08.02.2012, опубликовано в Интернет 20.03.2012 по положительной рецензии д.т.н., доц. Иванова А.И. (Пенза).