Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 9, Пенза-2014, с. 11 (http://www.pniei.penza.ru/RV-conf/T9/C11)

ОЦЕНКА ДОСТОВЕРНОСТИ ГИПОТЕЗЫ НОРМАЛЬНОСТИ ЗАКОНА РАСПРЕДЕЛЕНИЯ ЗНАЧЕНИЙ РАССТОЯНИЙ ХЭММИНГА МЕЖДУ БИОМЕТРИЧЕСКИМИ КОДАМИ «СВОЙ» И «ЧУЖОЙ»

Чекалева Т.Ю., Безяев А.В., Фунтикова Ю.В. (Пенза)

Нейростевые преобразователи биометрия-код могут иметь стойкость к атакам подбора от 10^3 до 10^{12} при использовании ими рукописных биометрических паролей, состоящих из 5 букв. Прямая оценка столь высоких значений стойкости к атакам подбора затруднительна, так как предполагает наличие больших баз биометрических образов «Чужие».

Проблему создания больших тестовых баз биометрических образов «Чужие» снимает ГОСТ Р 52633.3-2011 "Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора". Стандарт рекомендует при оценках стойкости к атакам подбора пользоваться гипотезой нормальности распределения значений расстояний Хэмминга между кодом «Свой» и кодами «Чужие». В этом случае для статистически достоверных оценок достаточно выборки порядка 200 биометрических образов «Чужие». На такой выборке удается достаточно точно вычислить статистические моменты нормального закона распределения значений.

Очевидно, что гипотеза нормальности закона распределения значений расстояний Хэмминга будет обладать разной достоверностью для разных образов «Свой». В частности по данным Надеева [1] эта гипотеза оказывается не верна при корреляции разрядов кодов «Чужие» более 0.37.

Установим зависимость достоверности гипотезы нормальности по критерию хи-квадрат от стойкости биометрических образов «Свой» к атакам подбора. Для этой цели была использована среда моделирования «БиоНейроАвтограф». Полученные данные сведены в таблицу 1.

Пароль	Ввод данных. Графический планшет	Ввод данных. Монипулятор «МЫШЬ»	Стойкость к атакам подбора	Достоверность гипотезы
«Пенза»	«НЕТ»	«ДА»	$10^{2.7}$	0.61
«Пенза»	«ДА»	«НЕТ»	$10^{5.2}$	0.83
«Сура»	«НЕТ»	«ДА»	$10^{3.1}$	0.71
«Сура»	«ДА»	«НЕТ»	$10^{5.5}$	0.85
«Мокша»	«НЕТ»	«ДА»	$10^{3.6}$	0.72
«Мокша»	«ДА»	«НЕТ»	$10^{7.7}$	0.93

Литература:

1. Надеев Д.Н. Синтез функции для вычисления вероятности пропуска «Чужого» по статистическим параметрам зависимых кодов-откликов «Чужой». Пенза-2012, Том 8, с. 8-9, Трудов конференции «БИТ»

Материал поступил 10.05.2013, публикуется по положительной рецензии д.т.н. Малыгина А.Ю.