Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 8, Пенза-2012, С 22-26 (http://пниэи.рф/activity/science/BIT/T8-p22.pdf)

ВВЕДЕНИЕ ДОПОЛНИТЕЛЬНОЙ ИЗБЫТОЧНОСТИ ДЛЯ ЗАЩИТЫ ПАРАМЕТРОВ ПРЕОБРАЗОВАТЕЛЕЙ БИОМЕТРИЯ-КОД ОТ ПОПЫТОК ИССЛЕДОВАНИЯ

Майоров А.В. (г. Пенза)

Нейросетевые преобразователи биометрия-код [1] используются для преобразования нечетких биометрических параметров различного качества в некоторый код доступа заданной длины. Для преобразователя биометрия-код (ПБК) функция преобразования может быть записана с помощью матричных и векторных операций (здесь и далее в формулах) следующим образом [2]:

$$y = \mathbf{F}(x) = \mathbf{f}(W_{[C]}(x+b)), \quad (1)$$

где W – матрица весов нейронов;

C – битовая матрица признаков использования j-го параметра для формирования отклика i-го нейрона;

x – вектор значений входных параметров;

b – вектор смещений "Все чужие";

f – вектор нелинейных функций нейронов;

y – вектор откликов (выходной код, код доступа).

После обучения преобразователя биометрия-код для последующего выполнения преобразования сохраняется тройка параметров (W,C,**b**).

Качество входных примеров биометрических образов для разных пользователей и биометрических технологий может значительно отличаться. Это связано с естественной нестабильностью воспроизведения человеком личной биометрии, погрешностью биометрических датчиков, психофизическим состоянием, конкретным биометрическим образом. Поэтому эффективная стойкость получаемого кода доступа значительно меньше идеальной (2^n). В значительной мере на ее снижение влияет наличие корреляции между биометрическими параметрами и их комбинациями. Так, например, для рукописного образа из 4-5 букв, эффективная стойкость выходного кода колеблется от 2^2 до 2^{12}, а для биометрии одного отпечатка пальца – от 2^4 до 2^8.

Параметры преобразования (W,C,**b**) могут использоваться злоумышленниками для упрощения атаки подбора входных параметров или выходного кода, например, через оценку энтропии выходного кода для образов "Все Чужие". Для противодействия атакам подбора необходимо повышать качество хэширования преобразователя биометрия-код таким образом, чтобы наблюдаемая атакующим энтропия выходного кода для биометрических образов "Все Чужие" должна стремиться к максимальному значению. Решением этой задачи является применение методов размножения ошибок. При этом изменяется как форма представления хранимых параметров, так и функция выполнения преобразования.

Один из способов защиты в случае, когда у злоумышленника имеется доступ к выходным параметрам ПБК и его откликам, но нет доступа к результатам промежуточных вычислений, заключается в повторении хэширования для выходного кода. Схема такого хэширования показана на рисунке 1.

Код, получаемый с преобразователя биометрия-код, подвергается

преобразованию с помощью криптографически стойкой хэширующей функции. В качестве дополнительных параметров хэширования могут использоваться любые коды, вычисленные ранее. Результат хэширования дополняется с помощью операции сложения по модулю 2 до требуемого выходного кода.

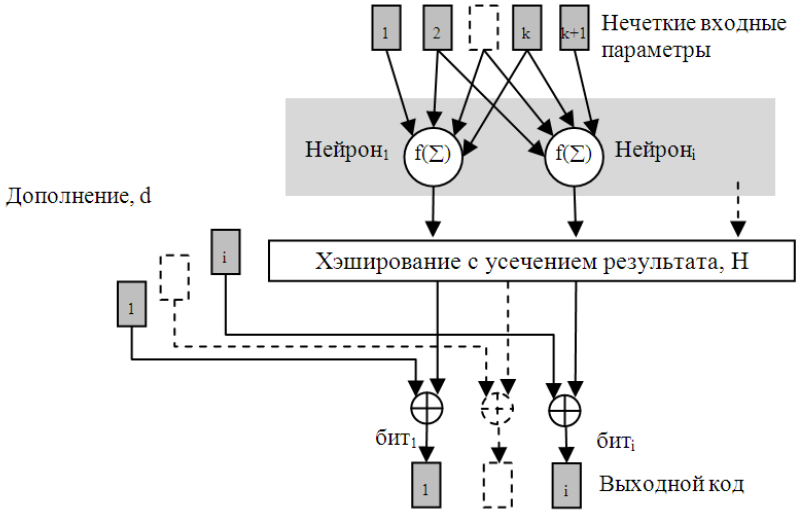

Рисунок 1

Формула (1) примет вид:

$$y = H(\mathbf{F}(x))\oplus d, \qquad (2)$$

где H – криптографически стойкая хэширующая функция;

d – двоичное число-дополнение.

Значение **F**(x) выбирают во время настройки ПБК случайным образом или как значение функции от выходного кода **F**(x) = H(y,...). Биты числа-дополнения вычисляют по формуле:

$$d_i = x_i \oplus H(F(x))_i, \qquad (3)$$

Предложенная схема значительно усложняет задачу злоумышленнику, не имеющему прямого доступа к промежуточному коду **F**(x), поскольку отклонение даже в одном бите этого кода приводит к значительным искажениям результата и не позволяет сделать вывод о близости подобранного параметра к эталонному значению.

Другим достоинством схемы является возможность связывания результата ПБК с внешними кодами, вычисленными ранее, например, в процессе мультибиометрической аутентификации.

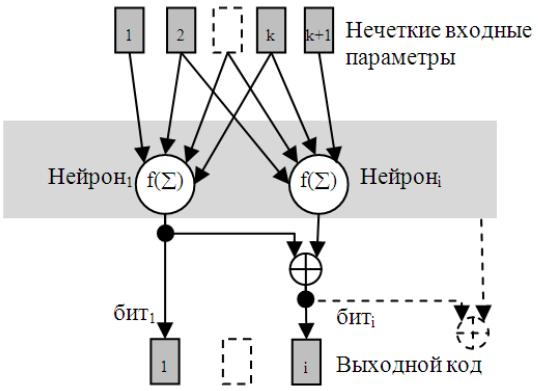

Рисунок 2

Схема защиты ПБК от исследования может быть выполнена и без

дополнительных хэширующих функций. В этом случае выполняется связывание значений откликов нейронов с ранее вычисленными.

В простейшем случае используется операция сложения по модулю 2 выхода i-го нейрона и i-1-го, вычисленного на i-1 шаге преобразования, как это показано на рисунке 2.

$$y_0 = 0,\ y_i = f(W[C_i](x_i + b_i)) \oplus y_{i-1}, \quad (4)$$

где y_0 – фиктивное начальное значение за пределами вектора y.

При реализации метода формула (1) на каждой итерации дополняется операцией сложения по модулю 2 с ранее вычисленным результатом, как это сделано в формуле (4). Таким образом, значение на выходе i-го нейрона оказывается связано со значениями, полученными ранее.

Подача параметров биометрического образа "Свой" не мешает получению правильного выходного кода. Однако, появление на выходе хотя бы одного нейрона значения, отличного от эталонного приводит к эффекту лавинообразного размножения ошибок, что затрудняет получение действительных значений выходного кода. Этот эффект проявляется при подаче биометрических параметров любого образа "Чужой" на вход настроенного ПБК.

Поскольку формула (4) отличается от исходной следует учесть это во время обучения. Для этого после обучения ПБК на выходном коде следует изменить знак всех весовых коэффициентов i-го нейрона путем умножения его на коэффициент s_i, вычисляемый по формуле (5):

$$s_i = -2 \cdot (y_i \oplus y_{i-1}) + 1 \quad (5)$$

Возможные модификации метода включают в себя замену y_{i-1} в формулах (4-5) на значение обратимых или необратимых дискретных функций от ранее вычисленных откликов нейронов $y_{1, \ldots, i-1}$.

Развитием способа защиты путем размножения ошибок является введение элемента случайности в процесс преобразования.

Для этого к m связям каждого нейрона ПБК, обученного предварительно, добавляется m_2 (где $m_2 > m$) новых связей с входными параметрами. Число добавляемых связей может быть фиксированным, а может выбираться случайным образом. Добавляемые связи размешаются в векторе C_i в случайном порядке. Номера добавляемых связей не должны дублировать имеющиеся у нейрона связи и должны выбираться по общему алгоритму распределения номеров связей по нейронам. Абсолютные значения соответствующих весовых коэффициентов, |W|, должны быть приближены к значениям "действительных" коэффициентов, получаемых во время обучения ИНС. Знаки добавляемых весовых коэффициентов должны выбираться таким образом, чтобы обеспечивать равновероятную смену значения отклика нейрона. Установка меньшей вероятности смены значения отклика позволяет наблюдать эффект отложенного возникновения ошибки для заданного подмножества образов "Все Чужие".

Функция преобразования биометрия-код модифицируется по одному из вариантов, первый из которых предполагает использование битовой маски, V_i, использования связей C_i при выполнении преобразования. Значение маски для образа "Свой" должно содержать "1" в разрядах, соответствующих исходным весам, и "0" для добавленных весов. Для образа "Чужой" значение маски случайно.

Во время преобразования маску V_i вычисляют как функцию от предыдущих откликов нейронов:

$$t = m + m_2,$$

$$V_i = d \oplus H(y_{1,\ldots,i-1})_{1,\ldots,t}, \quad (6)$$

где H(.) – функция хэширования, усеченная до t бит;

d – вектор бит числа-дополнения правильной маски V для образа "Свой". Значение d вычисляется во время обучения ПБК.

Более простая и быстрая формула (7) вычисления маски V_i требует согласования числа весовых коэффициентов и порядка их размещения с разрядами выходного кода, что менее удобно в общем случае.

$$V_i = y_{i-t,\ldots,i-1} \quad (7)$$

Общая формула выполнения преобразования биометрия-код для первого варианта представима как:

$$y_i = f(W_{[Ci \wedge Vi]}(x_i + b_i)) \quad (8)$$

Схема преобразования для этого варианта показана на рисунке 3.

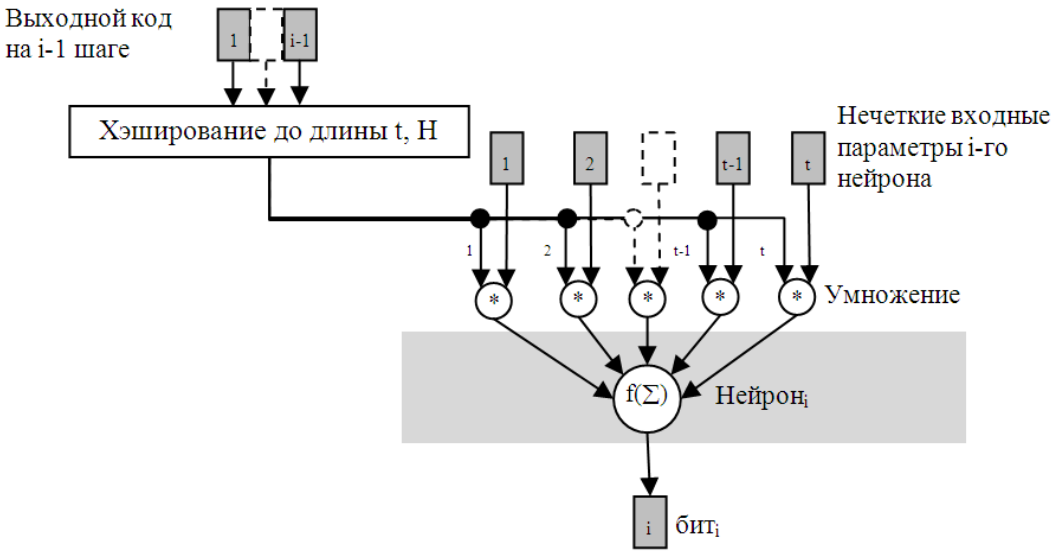

Рисунок 3

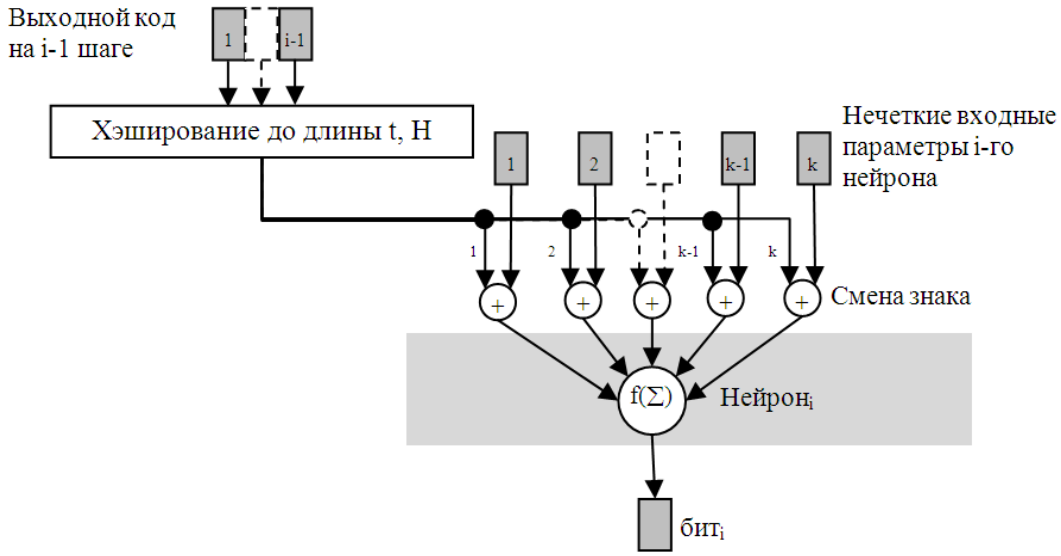

Рисунок 4

Второй вариант модификации алгоритма получения выходного кода представлен на рисунке 4 и, в отличие от первого варианта, предполагает использование добавленных весовых коэффициентов во

время каждого преобразования, взятых со знаком плюс или минус. Вектор знаков весовых коэффициентов S_i вычисляется как во время выполнения преобразования, так и во время дообучения ПБК по формуле:

$$S_i = 2\cdot(H(y_{1,\ ...,\ i-1})_{1,...,t}) - 1 \qquad (9)$$

Общее преобразование биометрия-код записывается как:

$$y_i=f(S_i\cdot W_{[Ci]}(x_i + b_i)) \qquad (10)$$

При этом во время настройки ПБК знаки "действительных" весовых коэффициентов изменяются таким образом, чтобы при их умножении на S_i для эталонных откликов $y_{1,\ ...,\ i-1}$ получались правильные значения весов. Добавленные веса изменяются таким образом, чтобы сумма их значений была близка к 0, т.е. не влияла на ошибку отказа по образу "Свой".

Проведенное имитационное моделирование показало, что предложенные методы размножения ошибок выходного кода и регуляции избыточности входных параметров значительно усложняют атаку подбора выходного кода ПБК с использованием неравномерности пространства кодов откликов и не дают злоумышленнику информации о необходимости смены направления движения во время атаки.

Литература:

1. ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.

2. ГОСТ Р 52633.5-2011 Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа.

Материалы поступили 01.03.2012, опубликовано в Интернет 20.04.2012 по положительной рецензии д.т.н., проф. Малыгина А.Ю. (Пенза).