ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ СРЕДСТВА АУТЕНТИФИКАЦИИ ПО СЕТЧАТКЕ ГЛАЗА

***С. А. ЗУБЕЦ*, П. М. БУЙ**

The algorithm of work of the authentification's mean on the retina of the eye is considered. The conclusion of the analytical formula for account of probability of the "another's" subject passing by the given authentification's mean from the first attempt is made. The example of account of probability of the "another's" passing from the first attempt is resulted at the given importance of the threshold of the affinity measure

Ключевые слова: средство аутентификации, радужная оболочка глаза, сетчатка глаза, вероятность пропуска «чужого» субъекта

Средство аутентификации – это программный модуль или аппаратно-программное устройство, которое обеспечивает проверку подлинности субъекта, т. е. устанавливает, является ли он тем, за кого себя выдает. Биометрические средства аутентификации отличаются тем, что предоставляемый субъектом биометрический признак никогда не будет полностью идентичен эталонному признаку.

Метод распознавания субъекта по сетчатке его глаза основан на уникальности данного рисунка. Факт наличия двух человек с одинаковой сетчаткой глаза является крайне маловероятным. Алгоритм сканирования радужной оболочки глаза состоит из следующих этапов: а) автоматический захват и фотографирование изображения; б) выделение сетчатки глаза на изображении; в) нормирование размеров изображения; г) получение сигнала от фотодатчиков; д) преобразование сигнала в цифровой вид;

е) сопоставление бинарных матриц, полученной по сканированному изображению, и хранящейся в базе данных средства аутентификации. Субъект будет положительно аутентифицирован, если данные бинарные матрицы будут считаться идентичными с долей совпавших битов, большей или равной заданному порогу меры близости. Порог меры близости – это критическое значение меры близости предоставляемого субъектом признака с эталонным, которое разделяет субъектов на «своих» и «чужих».

Вероятность пропуска «чужого» субъекта для данного аутентификатора вычисляется также, как и для средства аутентификации по радужной оболочке глаза:

$$P = \sum_{i=\mathrm{int}(A\cdot D)+1}^{A} \frac{A!}{i!\cdot(A-i)!}\cdot p^{i}\cdot q^{A-i}, \qquad (1)$$

где A – размер матрицы в битах; D – значение порога меры близости; $\mathrm{int}(A\cdot D)+1$ – доля совпавших битов в матрицах.

С использованием полученной аналитической формулы были рассчитаны вероятности пропуска данным средством аутентификации «чужого» субъекта в результате подбора последним биометрического аутентификатора с первой попытки при следующих значениях параметров: 1) объем данных, хранящихся в базе данных для одного человека – 40, 80, 120 и 160 байт/глаз; 2) значение порога меры близости –0,5, 0,51,…, 0,8 и 0,9; 3) вероятность совпадения и несовпадения одного бита в оцифрованном биометрическом аутентификаторе, представленным субъектом, с эталонным, хранящимся в базе данных средства аутентификации (p и q соответственно) – 0,5. Эта вероятность является показателем уровня защищенности средства аутентификации.

Например, вероятность пропуска «чужого» субъекта, равная 10^{-13}, достижима при значении порога меры близости, равном 0,7 при B = 40 байт/глаз. Для значения вероятности пропуска «чужого» субъекта, равной 10^{-4} при тех же размерах файла D = 0,59.

Таким образом, при сохранении заданной вероятности пропуска «чужого» субъекта средством аутентификации и при изменении одного из параметров остальные параметры неминуемо меняются, что привносит неуравновешенность в параметры этих биометрических средств аутентификации.