УДК 004.056.5 (075.8)

Евецкий В.Л.

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ДАННЫХ ЗА СЧЕТ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

Аннотация:

В статье кратко рассмотрен относительно новый способ защиты компьютерной информации – использование биометрической идентификации пользователя. При таком способе распознавания пользователя может быть использовано значительное количество признаков: особенности работы на клавиатуре, особенности работы с мышью и ряд других. При реализации биометрического способа идентификации представляет интерес сравнить ценность отдельных признаков для распознавания. Предлагается ввести в рассмотрение так называемый параметр распознавания q, который позволяет количественно оценить информативность признака для целей индивидуального распознавания, а также определить вероятность правильного распознавания пользователя по данному признаку или группе признаков.

Анотація:

У статті коротко розглянуто відносно новий спосіб захисту комп'ютерної інформації - використання біометричної ідентифікації користувача. При такому способі розпізнавання користувача може бути використана значна кількість ознак: особливості роботи на клавіатурі, особливості роботи з мишею і ряд інших. При реалізації біометричного способу ідентифікації представляє інтерес порівняти цінність окремих ознак для розпізнавання. Пропонується ввести в розгляд так званий параметр розпізнавання q, який дозволяє кількісно оцінити інформативність ознаки для цілей індивідуального розпізнавання, а також визначити ймовірність правильного розпізнавання користувача по даній ознаці або групі ознак.

Abstract:

The article briefly considered a relatively new way to protect computer information - the use of biometric user identification. Such method can use a large number of features: features of the work at keyboard, features of the work with the mouse, and others. When implementing a biometric identification method is of interest to compare the value of individual features for recognition. It is proposed to introduce the so-called recognition parameters q, which quantifies the the value of features for individual recognition, as well as to determine the probability of correct recognition on the basis of particular feature or group of features.

Стремление совершенствовать защиту данных от несанкционированного доступа привело к использованию в целях защиты относительно новых принципов, в частности использование принципов биометрической идентификации пользователя вместо (или в дополнение) к паролям, электронным жетонам и т.д. Так исследования [1-4] и др. показывают, что надежность идентификации пользователя можно существенно повысить при использовании уникальной манеры работы пользователя за персональным компьютером (ПК). Это и особенности работы пользователя на клавиатуре, и характерные приемы в использовании мыши, и особенности стиля и лексики электронных сообщений,

и другие особенности. Более того, систему можно настроить так, что как только проверенный и вошедший в систему пользователь покинет свое рабочее место, система будет проверять нового человека, занявшего это место, как нового пользователя со своими личными характеристиками. Таким образом, любой несанкционированный доступ к чужой рабочей среде, почте и другим данным может автоматически блокироваться.

Одним из основных и наиболее просто реализуемым вариантом есть «почерк» работы пользователя на клавиатуре. Этот почерк уникален. При работе на компьютере индивидуальность клавиатурного почерка (скорость, привычки использовать основную или дополнительную часть клавиатуры, характер «сдвоенных» нажатий клавиш и другие) позволяет с большой достоверностью опознать пользователя. Это сродни распознаванию по почерку радиста, который работает азбукой Морзе, или способности ценителя музыки различать на слух пианистов, исполняющих музыкальное произведение.

Для реализации распознавания пользователя по клавиатурному почерку могут использоваться различные признаки. Наиболее удобным для практического использования являются временные характеристики работы на клавиатуре: время нажатия каждой клавиши набираемого текста и интервал времени между нажатиями соседних клавиш. Контролируемые параметры существенно зависят от того, сколько пальцев использует при наборе пользователь, от характерных для пользователя сочетаний движений различных пальцев руки, от характерных движений рук при наборе и некоторых других. Как следует из ряда работ (например [2.3]), клавиатурный почерк конкретного пользователя обладает стабильностью.

Индивидуальное распознавание пользователя по клавиатурному почерку состоит в выборе соответствующего эталона из списка хранящихся в памяти эталонов, определения степени близости к этому эталону параметров почерка данного пользователя. Решение задачи распознавания пользователя сводится к решению задачи распознавания образов.

Как отмечалось, для распознавания можно использовать много различных признаков. Представляет интерес сравнить отдельные признаки с точки зрения их информативности для целей индивидуального распознавания и простоты реализации устройств распознавания.

Для оценки информативности отдельных признаков предлагается ввести в рассмотрение величину, которую целесообразно назвать **параметр распознавания q** .

Параметр распознавания

$$q = \frac{\sigma_{рп}}{\sigma_{оп}} \quad , \qquad (1)$$

где: $\sigma_{рп}$ - СКО разброса данного признака у разных пользователей,

$\sigma_{оп}$ - СКО разброса данного признака у отдельного пользователя.

Представляется очевидным, что данный признак тем более ценен для индивидуального распознавания, чем больший разброс он имеет у разных пользователей и чем более он стабилен у отдельного пользователя.

Можно показать, что условные вероятности правильного распознавания $P_{пр}$ и ложного распознавания $P_{л}$ определяются следующими соотношениями:

$$P_{пр} = 2\Phi(\frac{\delta_n}{\sigma_{pn}} q) , \quad (2)$$

$$P_{л} = 2\Phi(\frac{\delta_n}{\sigma_{pn}}) , \quad (3)$$

где: $\Phi(u) = \frac{2}{\sqrt{2}} \int_0^u e^{-\frac{s^2}{2}} ds$ - интеграл вероятности,

δ_n - пороговое значение при принятии решения по используемому признаку.

Рассчитанные вероятности правильного распознавания $P_{пр}$ при вероятности ложного распознавания $P_{л} = 10^{-2}$ для разных значений параметра распознавания q приведены в таблице 1.

Таблица 1

q	2	5	10	20	50	70	90	120	200
	0,02	0,06	0,1	0,29	0,55	0,68	0,77	0,87	0,99

Для определения значения параметра распознавания ***q*** различных признаков необходимо проведение статистического анализа экспериментальных данных, полученных из результатов работы операторов на ПК.

Практическая ценность предложенного для оценки информативности признака пара-метра распознавания ***q*** состоит в том, что знание его величины позволяет количественно оценить вероятность правильного распознавания конкретного пользователя при использовании данного признака (или группы признаков) при заданном уровне ошибки – вероятности ложного распознавания. Это позволяет провести сравнительный анализ информативности отдельных признаков для индивидуального распознавания, а также определить соответствующий набор признаков для распознавания пользователя с заданной степенью достоверности.

Литература:

1. *Иванов А.И.* Биометрическая идентификация личности по динамике подсознательных движений.- Пенза: Изд-во Пенз. гос. ун-та, 2000.

2. Софт@mail.ru Софт-клуб: Новости IT, 21.03.2012.

3. www. biometrics.ru

4. *Брюхомицкий Ю А*., Казарин М. Н. Метод биометрической идентификации пользователя по клавиатурному почерку.- Таганрог: Изд. ТРТУ, 2003, №4 (33), с.141-149.