ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.9

Н.А. Коляда[1], Ю.А. Чернявский[2]

АДАПТИВНАЯ ТЕХНОЛОГИЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

Предлагается оригинальная адаптивная технология распознавания пользователей компьютерных систем по клавиатурному почерку (КП). Синтезированная на ее основе идентификационная процедура использует адаптированные доверительные пороги и реализует принцип дифференциации в анализируемых текстах одинаковых слов рабочего словаря. Это позволяет существенно повысить уровень достоверности распознавания КП. Полученные экспериментальные данные показывают, что при доверительных вероятностях 92–98 % средние вероятности ошибок первого и второго родов в рамках созданной технологии не превышают порога 0,09.

Введение

Среди развиваемых в настоящее время биометрических идентификационных технологий особое место занимает технология аутентификации и идентификации пользователей компьютерных средств, основанная на анализе особенностей работы пользователя с клавиатурой, т. е. КП [1–4]. Интерес к этой технологии обусловлен, с одной стороны, заманчивой возможностью организации контроля доступа к компьютерным средствам полностью на программном уровне (без специальной аппаратуры), а с другой – достаточно высокой достоверностью идентификации (или верификации) пользователей, что обеспечивается уникальностью их КП.

Надежность процедур распознавания КП находится в прямой зависимости от мощности базового алфавита, объема рабочего словаря, измеряемых характеристик процесса нажатия и отпускания клавиш клавиатуры пользователем, количества учитываемых способов ввода им с клавиатуры отдельных слов (типов элементов КП), применяемых статистик для выработки эталонных (модельных) и формирования тестовых (верификационных) КП пользователей, ряда других характеристик.

Существующие подходы к созданию технологий распознавания КП базируются на той или иной гипотезе о законе распределения анализируемых временных характеристик процесса ввода информации пользователем с клавиатуры. Ввиду низкого уровня адекватности принимаемой гипотезы и реального распределения результирующие идентификационные процедуры не обеспечивают должной достоверности. Повышение данного показателя, в принципе, может быть достигнуто за счет расширения рабочего словаря. При этом, однако, резко возрастает трудоемкость алгоритмов распознавания.

Экспериментальные исследования показывают, что при создании систем контроля доступа по КП в качестве рабочих достаточно использовать словари, включающие слова из двух или трех символов базового алфавита. При этом для достижения высокой степени достоверности распознавания КП при приемлемых временных затратах гораздо более эффективным, чем расширение словаря, является применение адаптивных технологий, в рамках которых параметры формируемых моделей КП пользователей, а также решающего идентификационного правила принимают адаптивно-выбираемые значения [4–6]. К таким параметрам можно, в частности, отнести число типов элементов КП, объемы наборов значений вычисляемых статистик (адекватные типам элементов КП), характеристики распределений исследуемых временных интервалов и т. п.

В настоящей статье описывается обозначенный адаптивный подход к созданию систем идентификации КП (СИКП). В ней представлена технология распознавания КП, которая охватывает комплекс методов компьютерных процедур и программных средств, обеспечивающий генерирование КП пользователей в соответствии с разработанными концептуальными положениями, идентификацию и верификацию КП, а также автоматическую адаптацию системы к

санкционированному списку пользователей. Описанная оптимизационная методология затрагивает и проблемы качественного анализа предлагаемой идентификационной технологии.

1. Базовые положения

Определение 1. *Множество* $\boldsymbol{A} = \{c_k\}_{k=\overline{0,V-1}}$ *кодов* c_k *используемых символов в процессе анализа текстов, снимаемых с клавиатуры, будем называть рабочим алфавитом, а число* $V=|\boldsymbol{A}|$ *элементов множества* $\boldsymbol{A}$ *– объемом или мощностью алфавита.*

Определение 2. *Совокупность всех слов* (C_0, C_1, ..., C_{l-1})*, составленных из символов алфавита* ($C_i \in \boldsymbol{A}$; $i = \overline{0,l-1}$; $l \geq 2$)*, называется рабочим словарем СИКП.*

В предлагаемой технологии распознавания КП используется словарь $\boldsymbol{A}$, который состоит из двухсимвольных слов. При этом в анализируемых текстах рассматриваются пары смежных символов (C_0, C_1) $\in \boldsymbol{A} \times \boldsymbol{A}$, распределяемые по группам согласно присваиваемым им типам $T = T(C_0, C_1) \in \{0, 1, \ldots, N_T - 1\}$ (N_T – число типов пар).

Каждому символу с кодом $C \in \boldsymbol{A}$ в анализируемых текстах отвечают две тройки чисел-описателей: (1, C, $t_н$) и (0, C, $t_о$). Первая тройка описывает процесс нажатия (в момент $t_н$) клавиши, соответствующей коду C, а вторая – процесс отпускания этой клавиши (в момент $t_о$). Пусть в некотором текстовом массиве содержится пара (C_0, C_1) смежных символов с кодами C_0 и C_1. Обозначим через $A_{н,0}$ и $A_{н,1}$ адреса (порядковые номера) элементов массива, начиная с которых записаны тройки описателей символов C_0 и C_1, отвечающие нажатию соответствующих клавиш, а через $A_{о,0}$ и $A_{о,1}$ – адреса описателей процесса отпускания этих клавиш. Механизм присвоения паре смежных символов (C_0, C_1) искомого типа T базируется на вычислении опосредованного классификационного кода пары:

$$K = \frac{1}{3}\sum_{k=0}^{2} A_k \cdot B^k , \qquad (1)$$

где $A_0 = A_{о,0} - A_{н,0}$; $A_1 = A_{н,1} - A_{н,0}$; $A_2 = A_{о,0} - A_{н,0}$; B – основание системы счисления, используемой для формирования кодов вида (1), удовлетворяющее условию $A_{max} \leq 3B$; A_{max} – порог, ограничивающий сверху рост величин A_k. В процессе анализа текстовых файлов коды K помещаются в специальную таблицу (массив). При этом для пары символов (C_0, C_1) в качестве ее типа T принимается порядковый номер элемента этой таблицы, в который помещается классификационный код K данной пары.

Таким образом, реализуемая классификация пар (C_0, C_1) смежных символов в анализируемых текстах отвечает разновидностям комбинаций нажатия и отпускания клавиш на временном отрезке

$$[t_0; t_1](t_0 = t_{н,0}\,;\, t_1 = \max\{t_{о,0}, t_{о,1}\}), \qquad (2)$$

где $t_{н,0}$ – момент нажатия клавиши, отвечающей коду C_0; $t_{о,0}$ и $t_{о,1}$ – моменты отпускания клавиш, соответствующих C_0 и C_1.

В представляемой технологии роль базовой анализируемой измерительной характеристики выполняет длина $\tau = t_1 - t_0$ временного отрезка (2). При этом в основу применяемого решающего правила положено неравенство типа Чебышева

$$P\{(\tau - M_u(C_0, C_1, T))^2 \leq \mathrm{FCT}(u, p)\, D_u(C_0, C_1, T)\} \geq p/100 (\tau \in \boldsymbol{\tau}(C_0, C_1, T)), \qquad (3)$$

где $M_u(C_0, C_1, T)$ и $D_u(C_0, C_1, T)$ – соответственно среднее значение и дисперсия базовой временной характеристики, рассчитанные согласно формулам

$$M_u(C_0, C_1, T) = |\boldsymbol{\tau}_u(C_0, C_1, T)|^{-1} \sum_{\boldsymbol{\tau}_u \in \tau_u(C_0, C_1, T)} \tau_u \,; \qquad (4)$$

$$D_u(C_0, C_1, T) = \left|\tau_u(C_0, C_1, T)\right|^{-1} \sum_{\tau_i \in \tau_u(C_0, C_1, T)} (\tau_u - M_u(C_0, C_1, T))^2 \qquad (5)$$

на множестве $\boldsymbol{\tau}_u(C_0, C_1, T)$ всех значений, отвечающих одинаковым символьным парам (C_0, C_1) типа T в модельном текстовом файле u-го пользователя СИКП ($u \in \{0, 1, \ldots, U-1\}$; U – число пользователей); FCT(u, p) – коэффициент для расчета доверительного порога FCT(u, p) $D_u(C_0, C_1, T)$, адаптируемый к u-му пользователю при заданном (в процентах) уровне достоверности p; $\boldsymbol{\tau}(C_0, C_1, T)$ – множество значений временной характеристики τ, соответствующих парам (C_0, C_1) типа T в рассматриваемом верификационном тексте. Неравенство (3) применяется ко всем зарегистрированным символьным парам верификационного текста за исключением тех, для которых $\boldsymbol{\tau}_u(C_0, C_1, T) = \varnothing$.

При записи статистик (4) и (5) в массивы реализуется соответствие, при котором характеристикам $M_u(C_0, C_1, T)$ или $D_u(C_0, C_1, T)$ отвечают элементы, имеющие адрес (порядковый номер)

$$A = n_0 + n_1 V + TV^2, \qquad (6)$$

где n_k – порядковый номер кода C_k ($k = 0,1$) в списке *LCodeSimb* кодов символов рабочего алфавита. Таким образом, в рамках применяемого подхода для статистик (4) и (5) необходимы массивы, состоящие из $N_{\text{ЭС}} = N_T V^2$ элементов каждый.

В целях повышения быстродействия результирующей процедуры идентификации КП отображение подмножеств $\boldsymbol{\tau}_u(C_0, C_1, T)$ на наборы статистик применяется также для организации ускоренного анализа регистрируемых временных спектров. Это осуществляется с помощью связующего массива номеров пар смежных символов, в который для элементов спектра помещаются соответствующие им адреса вида (6). Использование указанных адресов связи обеспечивает простую и эффективную реализацию групповой статистической обработки элементов анализируемых временных спектров.

Отметим, что в условиях неопределенности закона распределения базовой временной характеристики и существенного его различия для разных пользователей, особенно при отсутствии классификации элементов КП по их типам, практически не удается достичь приемлемого уровня достоверности процедур распознавания. С учетом данного обстоятельства в неравенстве (3) коэффициент FCT(u, p) рассматривается как табулируемая функция двух аргументов: номера u пользователя системы и доверительной вероятности p. Оптимальные значения коэффициентов FCT(u,p) подбираются экспериментально в автоматическом режиме для каждого пользователя, имеющего право доступа к системе, при всех p из некоторого множества $\boldsymbol{P}$, например $\boldsymbol{P} = \{p_{min}, p_{min} + 1, \ldots, 100\}$, где p_{min} – нижнее пороговое значение доверительной вероятности (в процентах).

2. Процедура идентификации КП

Исходя из изложенных концептуальных положений, в качестве модельного КП u-го пользователя ($u = \overline{0, U-1}$) принимается следующая пара наборов (массивов) статистик:

$$\langle \boldsymbol{M}_u = \{M_u(C_0, C_1, T)\};\ \boldsymbol{D}_u = \{D_u(C_0, C_1, T)\} \rangle$$
$$(C_0, C_1 \in \boldsymbol{A};\ T \in \{0,1,\ldots,N_T - 1\}). \qquad (7)$$

Модели КП пользователей могут либо храниться в системе в виде выражения (7), либо каждый раз, по мере необходимости, генерироваться в рамках идентификационного процесса по содержащимся в системе модельным текстовым файлам с возможным их обновлением.

На базе изложенных концептуальных положений синтезирована идентификационная процедура, которая заключается в следующем.

1. Для анализируемого верификационного текстового файла формируются необходимый временной спектр (в массиве *TTIME_PAS_TextVerific*) с определением его объема – количества *NPAS_TextVerific* зарегистрированных пар (C_0, C_1) смежных символов, включая типы T, а также массив *AN_PAS_TextVerific* адресов связи вида выражения (6).

2. Полагается $u = 0$.

3. В массивы *AMEAN_MODEL* и *AVAR_MODEL* передаются компоненты $\boldsymbol{M}_u$ и $\boldsymbol{D}_u$ модельного КП u-го пользователя (см. (7)), а также фиксируется выбранный для него коэффициент FCT(u, p) (p – установленная доверительная вероятность для расчета доверительных порогов в неравенстве (3)).

4. Обнуляются счетчик N проверок базового критерия решающего правила, счетчик N^+ проверок с положительным исходом и переменная n.

5. Для элемента $\tau = TTIME\_PAS\_TextVerific[n]$ анализируемого временного спектра определяется адрес связи $A = AN\_PAS\_TextVerific[n]$ с соответствующими элементами массивов статистик (компонент КП u-го пользователя): $M_u(C_0, C_1, T) = AMEAN\_MODEL[A]$ и $D_u(C_0, C_1, T) = AVAR\_MODEL[A]$. Если при этом объем $|\boldsymbol{\tau}_u(C_0, C_1, T)|$ выборки $\boldsymbol{\tau}_u(C_0, C_1, T)$, по которой вычислены $M_u(C_0, C_1, T)$ и $D_u(C_0, C_1, T)$, не превышает установленного нижнего порога, то N наращивается на 1 и осуществляется переход к очередному шагу алгоритма, а иначе – к шагу 7.

6. Проверяется неравенство

$$(\tau - M_u(C_0, C_1, T))^2 \le \mathrm{FCT}(u, p)\cdot D_u(C_0, C_1, T), \tag{8}$$

и в случае его выполнения N^+ увеличивается на 1.

7. Производится наращивание переменной n, и при $n \ne NPAS\_TextVerific$ осуществляется переход к шагу 5. По достижении равенства $n = NPAS\_TextVerific$ вычисляется верификационная вероятность: $P_{\text{вериф}, u} = N^+ / N$, наращивается u и в случае $u \ne U$ осуществляется переход к шагу 3, а при $u = U$ – к очередному шагу.

8. Находится u^* такое, что

$$P_{\text{âåðèô},u^*} = \max\{P_{\text{âåðèô},u} \mid u = \overline{0,U-1}\}. \tag{9}$$

Если $P_{\text{âåðèô},u^*} \ge P_{\text{дов}} = p / 100$, то принимается решение, что тестируемый текст принадлежит u^*-му пользователю. В противном случае фиксируется факт несоответствия тестируемого текста с зарегистрированными в системе моделями КП пользователей.

Заметим, что тестовое неравенство (8) в сформулированном алгоритме применяется ко всем элементам анализируемого временного спектра. Это соответствует тотальному критерию решающего правила. В рамках предлагаемого подхода можно также использовать групповой критерий, при котором применяется тестовое неравенство вида

$$(M(C_0,C_1,T) - M_u(C_0,C_1,T))^2 \le FCT(u,p)\, D_u(C_0,C_1,T), \tag{10}$$

где $M(C_0,C_1,T)$ – выборочное среднее значение величины τ, рассчитанное на множестве $\boldsymbol{\tau}(C_0,C_1,T)$ (см. выражение (3)).

Приведенный идентификационный алгоритм тривиальным образом трансформируется в верификационную версию. Для этого достаточно удалить из алгоритма циклическую конструкцию по переменной u, включая равенство (9), обеспечив проверку соответствия исходного текста модельному КП лишь одного пользователя системы (с заданным номером u).

3. Результаты апробации идентификационной процедуры

На базе представленной адаптивной технологии распознавания КП в настоящее время разработана СИКП, которая апробирована на реальной распределенной информационной системе. В табл. 1 и 2 приведены экспериментальные результаты, полученные для $U = 8$ пользователей при доверительных вероятностях $p = 92, 95, 98$ % с применением в процедуре сравнения модельного и верификационного текстов соответственно тотального и группового критериев (см. выражения (8), (10)). В таблицах для каждого пользователя указаны адаптированные значения коэффициента FCT(u, p), а также отвечающие им средние верификационные вероятности $\overline{P}_{\text{âåðèô},u}$, веро-

ятности $\alpha = \alpha(u)$ ложного отказа пользователю (с номером u) в доступе к системе (ошибки первого рода) и вероятности $\beta = \beta(u)$ ошибочного санкционирования допуска пользователя к системе (ошибки второго рода). Требуемая оптимизация СИКП выполнена на основе тестовых наборов $\boldsymbol{F_u} = \{F_u(v)\}_{v=\overline{0,V_u-1}}$ текстовых файлов $F_u(v)$, принадлежащих соответствующим пользователям (V_u – количество файлов u-го набора; $u = \overline{0,U-1}$). Необходимые статистики рассчитывались по формулам

$$\overline{P}_{\text{âåðèô},u} = \frac{1}{V_u}\sum_{v=0}^{V_u-1} P_{\text{âåðèô},u}\{F_u(v)\}; \tag{11}$$

$$\alpha(u) = N_1(u) / V_u; \tag{12}$$

$$\beta(u) = N_2(u) / \sum_{u' \neq u} V_{u'}, \tag{13}$$

где $P_{\text{âåðèô},u}\{F_u(v)\}$ – верификационная вероятность (см. п. 7 в разд. 2), полученная для u-го пользователя на текстовом файле $F_u(v)$; $N_1(u)$ и $N_2(u)$ – количество зарегистрированных для u-го пользователя случаев ошибок первого и второго родов соответственно.

Таблица 1

Результаты адаптации процедуры распознавания КП
с применением тотального критерия сравнения текстовых файлов

Порядковый номер пользователя, u	Результаты адаптации при заданных значениях доверительной вероятности p, %											
	p = 92				p = 95				p = 98			
	FCT	$\overline{P}_{\text{âåðèô},u}$	α	β	FCT	$\overline{P}_{\text{âåðèô},u}$	α	β	FCT	$\overline{P}_{\text{âåðèô},u}$	α	β
0	2,5	93	0,091	0,017	4,5	97	0,000	0,035	8,5	98	0,091	0,026
1	2,5	92	0,091	0,035	4,5	96	0,000	0,078	10,5	98	0,091	0,130
2	3,5	94	0,091	0,095	6,5	97	0,000	0,096	12,5	99	0,000	0,069
3	3,5	94	0,091	0,096	4,5	96	0,091	0,069	10,5	98	0,091	0,183
4	3,5	95	0,000	0,079	4,5	96	0,000	0,026	11,5	98	0,083	0,087
5	4,5	93	0,083	0,026	7,5	95	0,166	0,026	24,5	97	0,166	0,298
6	3,5	94	0,090	0,104	4,5	95	0,182	0,069	13,5	99	0,091	0,383
7	3,5	95	0,000	0,017	4,5	96	0,000	0,017	9,5	98	0,000	0,026

Таблица 2

Результаты адаптации процедуры распознавания КП
с применением группового критерия сравнения текстовых файлов

Порядковый номер пользователя, u	Результаты адаптации при заданных значениях доверительной вероятности p, %											
	p = 92				p = 95				p = 98			
	FCT	$\overline{P}_{\text{âåðèô},u}$	α	β	FCT	$\overline{P}_{\text{âåðèô},u}$	α	β	FCT	$\overline{P}_{\text{âåðèô},u}$	α	β
0	2,5	96	0,000	0,026	2,5	96	0,000	0,0087	6,5	98	0,000	0,043
1	2,5	95	0,091	0,078	3,5	96	0,091	0,061	6,5	99	0,000	0,078
2	2,5	96	0,000	0,0435	5,5	98	0,000	0,061	16,5	99	0,091	0,087
3	3,5	97	0,091	0,178	4,5	97	0,091	0,119	7,5	99	0,091	0,089
4	2,5	97	0,000	0,0173	5,5	99	0,000	0,052	7,5	100	0,000	0,026
5	2,5	97	0,000	0,0198	5,5	99	0,000	0,059	7,5	100	0,000	0,029
6	2,5	96	0,182	0,035	2,5	96	0,182	0,017	5,5	98	0,182	0,035
7	4,5	87	0,182	0,485	7,5	88	0,182	0,515	13,5	89	0,454	0,504

Отметим, что в рамках проведенного тестирования фиксация ошибки первого рода в результате применения к $F_u(v)$ идентификационной процедуры происходит в случае невыполнения условия

$$P_{\text{âåðèô},u}\{F_u(v)\} \geq p/100. \tag{14}$$

Что касается ошибки второго рода, то ее фиксация для u-го пользователя происходит всякий раз, когда обнаруживается верификационный файл $F_{u'}(v')$ ($u' \in \{0, 1, \ldots, U-1\}$; $v' \in \{0, 1, \ldots, V_{u'}-1\}$), такой, что $u \neq u'$ и

$$P_{\text{âåðèô},u}\{F_{u'}(v')\} \geq p/100. \tag{15}$$

В процессе осуществляемой оптимизации СИКП в качестве искомых коэффициентов для расчета доверительных порогов в (8) и (10) принимаются наименьшие значения FCT(u, p), при которых вероятности $\alpha(u)$ и $\beta(u)$, вычисленные согласно (12) и (13), удовлетворяют следующему ограничительному условию минимизирующего типа:

$$\begin{cases} \alpha(u) \leq T_{min}(u); \\ \beta(u) \leq T_{min}(u) + d, \end{cases} \tag{16}$$

где $T_{min}(u)$ и d – подбираемые экспериментально (в автоматическом режиме) минимально возможные порог и неотрицательная константа. Если условию (16) удовлетворяет более одной пары $\langle\alpha(u), \beta(u)\rangle$, то искомой считается пара с минимальной суммой $\alpha(u) + \beta(u)$.

Как видно из выражений (8) и (10), увеличение FCT(u, p) ведет к возрастанию верификационных вероятностей $P_{\text{âåðèô},u}\{F_u(v)\}$, а значит, ввиду (14), – к убыванию $\alpha(u)$. При этом, однако, обнаруживается тенденция к возрастанию вероятностей $P_{\text{âåðèô},u}\{F_{u'}(v')\}$ (если $u' \neq u$), а следовательно, и $\beta(u)$. Таким образом, требование одновременной минимизации $\alpha(u)$ и $\beta(u)$ противоречиво, и именно поэтому оно заменено на более гибкое оптимизационное условие (16).

Представленные в таблицах результаты апробации СИКП получены в автоматическом адаптационном режиме с использованием 8 модельных (по числу пользователей) и 90 верификационных файлов. Объемы V_u наборов F_u верификационных файлов для пользователей составляют $V_u = 11$ ($u \neq 5,7$), $V_5 = V_7 = 12$. В реализуемой конфигурации процедуры сравнения модельного и верификационных текстовых файлов проверка базового критерия, как тотального, так и группового, проводилась с исключением символьных пар, для которых модельные выборочные статистики (среднее значение и дисперсия) рассчитаны по выборкам объемом, не превышающим 11. Как показывает эксперимент, это повышает уровень достоверности распознавания КП.

Описанная оптимизация СИКП с применением выражения (16) приводит к соответствующей минимизации вероятностей $\alpha(u)$ и $\beta(u)$ ошибок первого и второго родов для каждого пользователя. Поэтому она обеспечивает и адекватную минимизацию вероятностей A и B ошибок первого и второго родов для идентификационного режима, охватывающего всех U пользователей системы. Данные, представленные в табл. 3, полностью согласуются с этим утверждением.

Качественный анализ предложенного механизма регулирования характеристик достоверности распознавания КП посредством изменения коэффициентов FCT(u, p) в выражениях (8) и (10) целиком подтверждает гибкость и эффективность этого механизма. Полученные экспериментальные данные свидетельствуют о том, что внедрение адаптивных методов в технологии распознавания пользователей по КП является весьма действенным и перспективным средством повышения их надежности и конкурентоспособности.

Таблица 3

Результаты идентификации пользователей по КП (u = 0, 1, …, 8)

Заявляемый номер пользователя, u	Тотальный критерий						Групповой критерий					
	p = 92		p = 95		p = 98		p = 92		p = 95		p = 98	
	$u_И$	$p_И$	$u_И$	$p_И$	$u_И$	$p_И$	$u_И$	$p_И$	$u_И$	$p_И$	$u_И$	$p_И$
0	0	93	0	96	0	98	0	97	0	97	0	99
1	8	96	8	97	1	99	1	98	1	98	1	98
2	2	95	2	98	2	99	2	94	2	96	2	100
3	3	95	3	97	3	99	3	93	3	97	3	98
4	4	93	4	95	4	98	4	99	4	99	4	99
5	5	94	5	97	5	99	5	96	5	98	5	100
6	6	97	6	98	6	100	6	98	6	100	6	100
7	7	93	7	94	7	99	7	100	7	100	7	100
8	8	97	8	99	8	99	8	99	8	99	8	100

Заключение

Основные результаты представленной в настоящей статье разработки по проблеме создания адаптивных технологий распознавания пользователей по КП состоят в следующем.

1. В рамках решающего правила, базирующегося на неравенствах типа Чебышева, предложена оригинальная идентификационная технология, ключевым компонентом которой является адаптация применяемого набора доверительных порогов к санкционированному списку пользователей.

2. Разработана модель КП пользователя, которая позволяет осуществлять дифференциацию одинаковых слов в текстах по типам комбинаций нажатий и отпусканий клавиш на временных отрезках ввода слов. Соответствующее группирование слов повышает уровень адекватности принадлежащих одному и тому же пользователю верификационных текстов и моделей КП, а значит, и достоверность распознавания КП.

3. На основе предложенных адаптационных принципов синтезирована процедура распознавания КП, пригодная для работы как в верификационном, так и в идентификационном режимах. Приведены результаты тестовых испытаний данной процедуры на вычислительной системе с 10 пользователями.

Представленная работа выполнена в рамках ГКПНИ «Инфотех».

Список литературы

1. Рыбченко, Д.Е. Анализ клавиатурного почерка аппаратом нечетких множеств для целей ограничения доступа и аудита / Д.Е. Рыбченко, А.И. Иванов // Специальная техника средств связи. Сер. «Системы, сети и технические средства конфиденциальной связи». – 1996. – Вып. 1. – С. 116–119.

2. Завгородний, В.В. Идентификация по клавиатурному почерку / В.В. Завгородний, Ю.Н. Мельников // Банковские технологии. – 1998. – № 9. – С. 68–72.

3. Радыно, Н.Я. Алгоритм идентификации пользователя компьютера по набору фиксированной фразы на клавиатуре / Н.Я. Радыно // Весці НАН Беларусі. Сер. фіз.-мат. навук. – 2002. – № 3.– С. 97–103.

4. Коляда, Н.А. Адаптивная технология идентификации по клавиатурному почерку / Н.А. Коляда, Ю.А. Чернявский // Управление защитой информации. – 2006. – Т. 10, № 1. – С. 50–53.

5. Иванов, А.И. Биометрическая идентификация личности по динамике подсознательных движений / А.И. Иванов. – Пенза: Изд-во Пензенского государственного университета, 2000. – 188 с.

6. Минченко, Л.И. Биометрические средства идентификации и аутентификации пользователей распределенных информационных систем / Л.И. Минченко, Н.Я. Радыно, Ю.А. Чернявский // Материалы 1-й Междунар. конф. IST'2002. Ч. 2. – Минск, 2002. – С. 75–76.

7. Корн, Г. Справочник по математике (для научных работников и инженеров) / Г. Корн, Т. Корн. – М.: Наука, 1973. – 832 с.

Поступила 05.09.06

[1]*Институт прикладных физических проблем им. А.Н. Севченко БГУ, Минск, Курчатова, 7 e-mail: kolyada@bsu.by*

[2]*Белорусский государственный университет информатики и радиоэлектроники, Минск, П. Бровки, 6 e-mail: bsuir@bsu.by*

N.A. Kolyada, Ju.A. Chernyavsky

ADAPTIVE TECHNOLOGY OF USER IDENTIFICATION ON KEYBOARD HANDWRITING

The original adaptive technology of computer system user recognition on keyboard handwriting (KH) is offered. The identification procedure uses adapted confidential thresholds and realizes a principle of differentiation in analyzed texts of identical words of the working dictionary. It allows to increase essentially a level of reliability of KH recognition. The obtained experimental data show, that at confidential probabilities 92–98 % the average probabilities of mistakes I and II types within the framework of the created technology do not exceed a threshold 0,09.