2017 IEEE Dynamics of Systems, Mechanisms and Machines (Dynamics) (Omsk, Russia)
14 Nov–16 Nov 2017

Users' Identification Through Keystroke Dynamics Based on Vibration Parameters and Keyboard Pressure

Alexey E. Sulavko
Omsk State Technical University,
Omsk, Russia
sulavich@mail.ru

Alexander V. Eremenko
Omsk State Transport University,
Omsk, Russia
4eremenko@gmail.com

Alexander A. Fedotov
Omsk State Transport University,
Omsk, Russia
fedotov1609@gmail.com

***Abstract*—The paper considers an issues of protecting data from unauthorized access by users' authentication through keystroke dynamics. It proposes to use keyboard pressure parameters in combination with time characteristics of keystrokes to identify a user. The authors designed a keyboard with special sensors that allow recording complementary parameters. The paper presents an estimation of the information value for these new characteristics and error probabilities of users' identification based on the perceptron algorithms, Bayes' rule and quadratic form networks. The best result is the following: 20 users are identified and the error rate is 0.6%.**

***Keywords*—Keys pressure, keyboard vibration, wide artificial neural networks, correlation between biometric attributes, probability density.**

I. INTRODUCTION

Nowadays IT penetration into the society is an active process. A growing number of web-services appears. Many countries tend to build an electronic government to provide services to their citizens. The level of confidentiality to such services must be the highest. But the majority of confidential information leaks, and cyber attacks happen due to the web services. The world number of leakage annually grows [1]. The available estimations of the world financial losses due to these incidents impress, they account for $375-575 billion [2] annually. Organizations of different level deploy biometric security systems to decrease these losses. As of October 2016 biometric authentication is used by 57% of enterprises [3].

Statistic biometric images (a fingerprint or an iris) are not private, so they can copied by making a material or digital model (for remote authentication). Private biometric images contain a secret (a password) so they can potentially provide a higher level of protection. They include personal keystroke dynamics disclosed while typing a password phrase. A weak point of the method of authentication through the keystroke dynamics is relatively low reliability of decisions made as the probability of false rejection error (FRR) and false access rate error are too significant to use this method in practice [4]. This work investigates the issue of increasing the reliability of personal recognition through keystroke dynamics by using additional characteristics that describe the dynamics of text typing: key pressure parameters (pressure force) and keyboard vibration.

II. DEVELOPMENT OF A MODIFIED KEYBOARD FOR BIOMETRIC DATA CAPTURE

The experiments to be carried out need a keyboard that allow recording additional characteristics of the keystroke dynamics (the pressure and the vibration). Keyboard models with these functions are either single-piece test samples not available for making an order or have a form-factor that is not suitable for our purposes (a mobile device keyboard). At the same time the modern development tools for programmable electronic devices allow solving this task independently.

Arduino Uno R3 controller built on ATmega328 chip was selected as a platform to develop a software and hardware complex to record complementary characteristics of the keystroke dynamics. The chip of this controller converts the analog signal to a digital one using an integrated analog-digital converter and may be used for the development of interactive systems that manage different sensors and switches. The process of the development of the software and hardware complex consists of the following stages:

A keyboard layout is designed (Fig. 1 a);

Components are selected and purchased;

Engineering works are carried out.

A vibration sensor and 5 pressure sensors were connected to Arduino Uno R3. A force-measuring sensor Interlink 408

FSR was used to measure the force of pressing a key. The force-measuring sensor Interlink 408 FSR is a force-measuring resistor manufactured as a low-profile thin passive component, its resistance is proportional to the force applying to its surface.

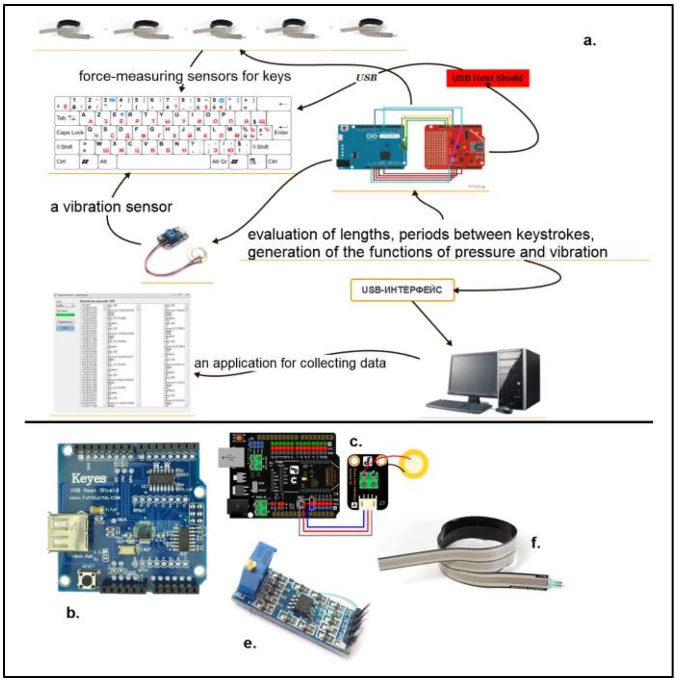
a.
force-measuring sensors for keys
USB
USB Host Shield
a vibration sensor
evaluation of lengths, periods between keystrokes,
generation of the functions of pressure and vibration
USB-ИНТЕРФЕЙС
an application for collecting data
Keyes
b.
c.
e.
f.

Fig. 1. a. a structural pattern of the software and hardware complex to record keystroke dynamics; b. a force-measuring resistor Interlink 408 FSR; c. USB Host Shield module to connect USB devices to Arduino controller; d. connection of the piezoelectric vibration sensor to the Arduino Uno board; f. a module for amplifying an analog signal based on an operational amplifier LM358.

In an idle mode the resistance exceeds the value of 1 milliohm and varies from 100 kilohm to several hundreds of ohm depending on the power of pressure on the sensor surface. To obtain the data on the vibration of the keyboard while typing a text the piezoelectric vibration sensor Analog Piezo Disk Vibration Sensor from DFRobot is used. This sensor can detect even minor vibration. When the piezoelectric element is connected to the microcontroller it outputs a signal that is proportional to the vibration amplitude. The USB Host Shield module is used to identify key codes and the pressure moments. It is designed to connect HID-devices and emulation of their work in the OS. The adjustable module based on the operational amplifier LM358 is used to enhance an analog signal. The keyboard Logitech K120 is connected to the Arduino Uno R3 module through USB Host Shield. The keyboard body was opened and the pressure sensors were mounted under the key rows (Fig.2).

The sampling rate for Arduino Uno R3 is 3000 Hz but as it samples 6 channels (sensors) one-at-time, the actual sampling rate for every recording signal is 500Hz. It is necessary to focus on the highest possible speed of key stroking to evaluate the most meaningful frequency of signals that are generated while typing a text. In 2005 Barbara Blackburn was credited by the Guinness Book of Records as the fastest English language typist in the world using the Dvorak simplified keyboard (a variant of a keyboard layout that provides the higher speed of typing a text in comparison with the traditional QWERTY layout). Barbara Blackburn was typing with the average speed of 150 words per minute for 50 minutes, sometimes the speed increased to 170 words per minute, and for a short period of time her speed was 212 words per minute. In the English language the average word size is 5.2 letters, but WPM (a number of Words Per Minute) is sometimes taken as 5 symbols. In other countries the typing speed is measured in CPM (Characters Per Minute) or in SPM (Strokes Per Minute). Thus, Barbara Blackburn's record was 750 characters per minute. According to other researches, the standard typing speed is 150-220 characters per minute for the QWERTY-keyboard, a good typing speed is 250-330 characters. The best typing speed for a keyboards mentioned in open sources correlates with the frequency of 12.5 Hz, a standard speed correlates with 2.5Hz. According to Nyquist–Shannon–Kotelnikov theorem the sampling rate must be twice the frequency of being sampled. It follows, that the sample rate of 25 Hz is sufficient to record all frequency changes in a key stroking manner.

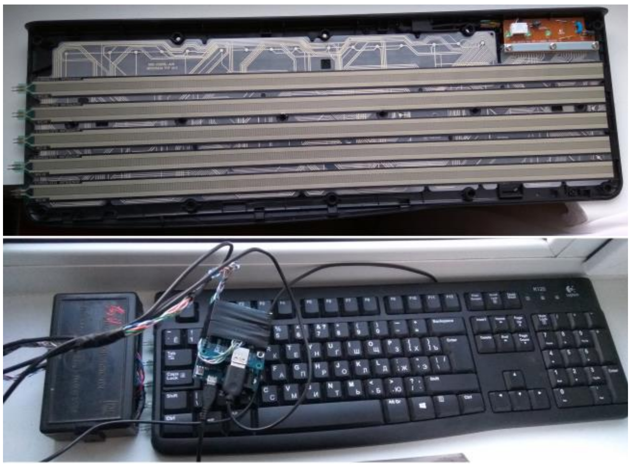

Fig. 2. Layout of sensors and the exterior of the keyboard.

To process data obtained from the keyboard and complementary sensors a software module was written on C#.

III. KEY STROKE MANNER ANALYSIS

A. Database of biometrical samples

A group of 100 test person was used to collect biometrical samples. The test persons were selected in a certain way to provide the equal number of representatives of all types of temperaments (melancholic, phlegmatic, sanguine and choleric) that was proved by Eysenck's tests (it is known that the type of temperament influences the characteristics of the key stroking manner). Ever test person inputs a password phrase «Let me access the information» at least 120 times using the developed keyboard. We call every block of data generated every time the text or the password phrase is input as a key stroke sample.

B. Identification attributes

Every sample was converted into a vector of attribute values (a sample of a key stroke manner). An attribute is an identification descriptor, a certain physical value that characterizes an operator. By their physical sense the attributes being analyzed in this paper may be divided into several conventional categories presented in the Table 1.

The basic attributes of the key stroke manner are the holding time and pauses between key strokes [4, 5] (the categories 1.1-1.2, Table 1). Another attribute that is considered in research works is the frequency or time of pressing a pair of keys simultaneously (overlap time) while typing a text or a password phrase [5, 6]. Sometimes a combination of several attributes into a cluster occurs, it describes an *n*-gram that is a sequence of *n* characters. This cluster may include the holding time of n keys, n-1 pauses between key strokes, the time of holding 2, 3, n keys simultaneously.

When the key is held down many values of instant pressure on the key and instant vibration of the keyboard are recorded. Both average and maximum meanings of these values may be used as attributes. In this paper the maximum recording level of pressure and vibration on a key is to be tested (the attribute category 2.1-2.2, Table 1). The correlation between the average and maximum values of keystrokes is very significant (more than 0.9), and the difference between these values for test persons was less noticeable.

The present paper proposes to move from the time representation of the function of instant pressure on keys $p(t)$, and the function of keyboard vibration $vibro(t)$ to the frequency representation, their research and the search for dynamical characteristics based on the multiresolution analysis approach (attribute categories 3.1-3.2, Table 1). The function $p(t)$ describes the level of pressure on the keyboard when one or a group of keys is pressed (it analyzes the maximum values of pressure in a group of keys pressed simultaneously) in a moment of time t, the function $vibro(t)$ assigns the vibration value to the moment of time t.

These functions differ in the length that is why they are preliminary processed to one-time scale. In this regard the Fourier transform decomposes the functions $p(t)$ and $vibro(t)$, the amplitude and the frequencies of the first k harmonics are computed. Next step is to replace the harmonic frequencies of the scaled function with the frequencies of the corresponding harmonics computed for the scaled functions. At the next step the k harmonics with modified characteristics are passed through the inverse Fourier transform. Normalized functions are amplitude-frequency analyzed in the same manner as the functions of coordinates and stylus pressure while writing a signature in the paper [7]. The method of decomposing functions $p(t)$ and $vibro(t)$ applied is based on the discrete wavelet transform, and uses Mallat's algorithm to decompose initial signals into sequences of wavelet coefficients d_{jk} that describe the structure of the analyzed process in different scales j. In these researches Daubechies' D6 basis as in [7] was used.

The analyzed signals were sampled at a frequency of 500Hz therefore the highest possible frequency of the signal resulted from the frequency analysis is 250 Hz according to Nyquist–Shannon–Kotelnikov theorem. Table 2 shows calculations for 9 levels of decomposition of the signals used in the experiments. It has been discovered that the spectral range for the control signals of the signature is within 2…12.5 Hz. Thus, the major power of the signal must be concentrated in the 5th–7th decomposition levels. The physical meaning of wavelet transform coefficients may be treated as characteristics of the signal harmonics within a certain frequency range occurring in the signal in a certain period of time. These characteristics may be treated as values of the attributes from the categories 3.1-3.2. In total we have obtained 720 attributes for each of the functions $p(t)$ and $vibro(t)$, that account for 1440 attributes from each password phrase.

TABLE I. DESCRIPTION OF ATTRIBUTES OF KEYSTROKE DYNAMICS

№	**Attribute category**	**Brief description**	**The most relevant law of distribution**
1.1	Time of key held down	A time interval between events, when a certain key is held down and released (in milliseconds). Every key is associated with an attribute.	Normal
1.2	Pauses between keystrokes	A time interval between events when one key is held down and another key is held down (in milliseconds). Every pair of keys is associated with an attribute.	Lognormal
2.1	Pressure on keys	A pressure value that is measured while holding down a certain key. Every key is associated with an attribute.	Normal
2.2	Vibration while stroking keys	A value of keyboard vibration that is measured while holding down a certain key. Every key is associated with an attribute.	Normal
3.1	Wavelet parameters of pressure	Daubechies' D6 wavelet transform coefficients that are calculated based on the function of key pressure generated while inputting a sample of keystroke dynamics.	Laplace (double exponential)/ Normal
3.2	Wavelet parameters of vibration	Daubechies' D6 wavelet transform coefficients that are calculated based on the function of keyboard vibration generated while inputting a sample of keystroke dynamics.	Laplace (double exponential)/ Normal

TABLE II. SCALE AND FREQUENCY CHARACTERISTICS OF WAVELET COEFFICIENTS AT DIFFERENT LEVELS OF DECOMPOSITION

Level of decomposition	**Frequency range, Hz**	**Time resolution (scale), ms**
1	125–250	2
2	62.5–125	4
3	31.25–62.5	8
4	15.625–31.25	16
5	7.8125–15.625	32
6	3.90625–7.8125	64
7	1.953125–3.90625	128

8	0.9765625–1.953125	256

The most relevant laws of distribution for attribute values from the Table 1 are computed based on Pearson's chi-squared method.

C. Informative value of attributes

In order to understand whether supplementary attributes contain new information it is necessary to estimate the correlation dependence between the time of key held down, the pressure on the keys and the keyboard vibration arising when keys are pressed, as well as pauses between corresponding keystrokes. For this purpose it is sufficient to compute coefficients of paired correlation between corresponding blocks of samples of personal keystroke dynamics. Let us calculate these coefficients for all samples of all test persons, and build bar charts of relative frequencies of these coefficients (Fig.3).

As Figure 3 shows the correlation between attributes of different categories does not exceed 0.7 almost in all cases, and either matches low dependence according to Chaddock's scale or is absents at all in general. In several cases (no more than 15%) the dependence is moderate, rarely visible (less than 5%). The conclusion is the following: information in attributes from different categories is not duplicated, the information channels may be treated as low dependent.

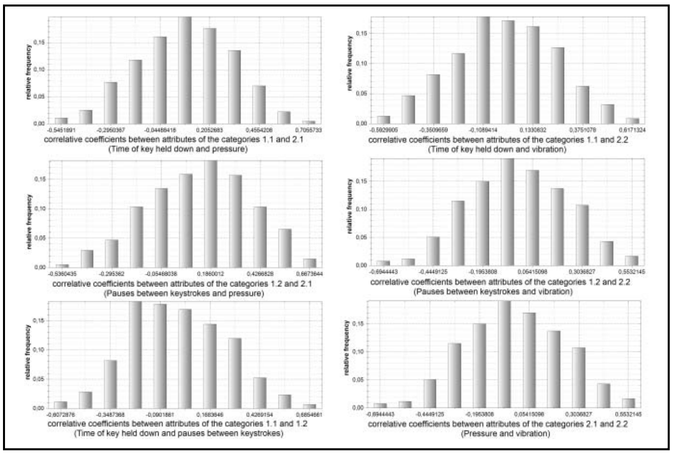

Fig. 3. Mutual dependence between attributes from different categories.

Let us also define the degree of dependence between the attributes from the category 3.1. For this purpose let us calculate the coefficients of paired correlation between coherent cutsets of the corresponding attributes. A cutsest is a set of attribute values (in analogy with a random value). Coherent cutsets of two attributes contain sequences of their values that are in phase that means the sequence order of samples in an attribute value array is the same for 2 cutsets. According to the results of estimation, the correlative mutual dependence for 720 attributes of the category sometimes exceeds 0.3 and matches the low dependence according to Chaddock's scale. The same result was obtained for attributes from the category 3.2. That is why the further increase in a number of wavelet coefficients is possible, but the time of processing these samples of keystroke dynamics will significantly increase if other attributes are used.

We can judge about the informative value of an attribute by the area of intersection for probabilities of its values that describe different people [8]. The intersection area $Sp_{ik}(A_j)$ for the probability-density function of the j^{th} attribute that characterizes the i^{th} test person and the probability-density function of the same attribute that characterizes the k^{th} test person is a sum of probabilities for the errors type I and type II, that is the probability of false recognition for the i^{th} and k^{th} test person based on the attribute A_j. For different test persons areas $Sp_{ik}(A_j)$ may significantly differ, the integral estimation of the informative value for all test persons may be obtained using the parameters of distribution of a value $Sp_{ik}(A_j)$ (Fig.4). Attributes with the highest informative values have the least mean value $Mx(Sp_{ik}(A_j))$ of the areas $Sp_{ik}(A_j)$, attributes with the lowest informative values have the highest values $Mx(Sp_{ik}(A_j))$ in contrast. The more the informative value of the attribute differs for different persons, the higher root-mean-square deviation $Sx(Sp_{ik}(A_j))$ of areas $Sp_{ik}(A_j)$. Attributes with high estimations $Sx(Sp_{ik}(A_j))$ have a high informative value for one test persons and a low informative value for other test persons (Table 3).

TABLE III. MEAN ESTIMATORS OF INFORMATIVE VALUE OF ATTRIBUTES

№	Attribute category	$Mx(Sp_{ik}(A_j))$	$Sx(Sp_{ik}(A_j))$
1.1	Time of key held down	0.62099	0.08352
1.2	Pauses between keystrokes	0.57107	0.11538
2.1	Pressure on keys	0.53589	0.10424
2.2	Vibration while stroking keys	0.80117	0.03526
3.1	Wavelet-parameters of pressure	0.77147	0.05706
3.2	Wavelet-parameters of vibration	0.78358	0.04579

Despite of a comparatively low mean estimator of the informative value of the attributes from the categories 3.1–3.2, the total potential of these attributes is high due to its large number. A password phrase consisting of 30-40 characters outputs 1440 attributes with preferably low mutual correlation according to Chaddock's scale for a reasonable period of time. Wavelet coefficients with high frequency have the highest informative value (Fig. 4). When passing to the following level of decomposition the timing resolution increases, and the frequency range goes down (Table 2), the highest total quantity of information about a typing person is contained in the high-frequency block of the functions $p(t)$ and $vibro(t)$. In total, the keyboard vibration has less information value than the pressure on key for the purpose of operator's recognition and authentication.

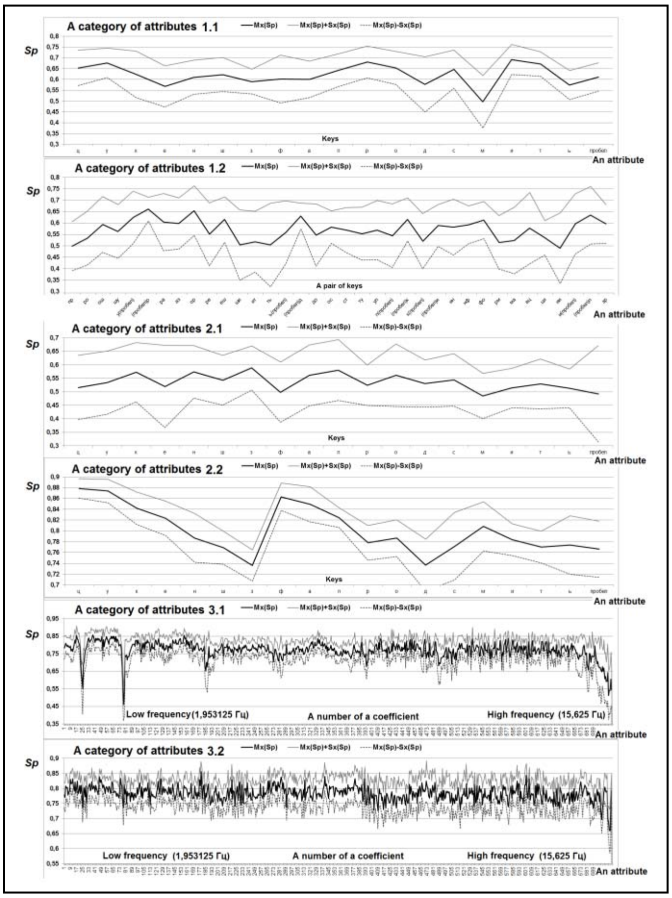

Fig. 4. Estimation of the informative value of the attributes by $Sp_{ik}(A_j)$ areas for 100 test persons.

III. Recognition of users via keystroke dynamics

There are two modes of recognition: identification and verification. In the first case the system defines a class an image belongs to among classes the system knows. In the second case an expected class is indicated and the algorithm of recognition defines whether the presented image belongs to this class (this principle is used in authentication systems). In the identification mode the number of errors increases when the number of images to be identified grows. In this work we identify 10 and 20 person simultaneously (a simulation experiment was carried out several times using different combinations of test persons, the error probabilities were averaged).

A. Identification of users via keystroke dynamics

The algorithm of personal identification may be used via the method of successive Bayes hypotheses formula, (1) [9] that suggests the computation of integral posterior probabilities of the hypotheses for a certain number of steps equal to a number of attributes using the formula (1). Every hypothesis presumes the presented sample of keystroke dynamics belongs to a certain user that is every hypothesis is associated with a certain user's sample. At every step posterior probability calculated at a previous step is a prior probability for the next step. The probability density of the next attribute inputs as conditional probability.

$$P(H_i|A_j) = \frac{P_{j-1}(H_i|A)P(A_j|H_i)}{\sum_{i=1}^{n} P_{j-1}(H_i|A)P(A_j|H_i)} \qquad (1)$$

where $P(A_j|H_i)$ is conditional probability of the hypothesis H_i that says the presented data belong to the sample of the i^{th} test person and is equal to the probability density of the value of the j^{th} attribute, $P_j(H_i /A)$ is a posterior probability of the i^{th} hypothesis calculated at the j^{th} step. All hypotheses (subjects) are considered equally probable at the first step, that is $P_0(H_i/A) = 1/n$, where n is a number of identifying hypotheses.

Templates of the test persons (the calculation of the parameters of the attribute density) were generated based on 21 samples of a password phrase from every test person, the same number the state standard GOST R 52633.5-2011 recommends using for training neural networks (the perceptron networks). Other samples were used for identification. In total more than 10 000 experiments were carried out. The test validity was more than 0.99 when the confidential interval of probability was 0.003. The following results were obtained:

- When 10 test persons are identified in a space of only basic attributes (the categories 1.1-1.2) the average error probability is 0.004.
- When 20 test persons are identified in a space of only basic attributes (the categories 1.1-1.2) the average error probability is 0.025
- When 10 test persons are identified in a space of basic and supplementary attributes (all categories), the average error probability is 0.002.
- When 20 test persons are identified in a space of basic and supplementary attributes (all categories), the average error probability is 0.006.

B. User's verification via keystroke dynamics

The state standard GOST R 52633.5-2011 recommends using a single-layer or two-layer artificial neural network for biometric authentication. The first layer enhances data, the second layer acts as an error-correcting code. In our work we use a single-layer neural network [10]. Neurons' weights are calculated deterministically using the formula:

$$\mu_i = |\mathrm{E}_{ч}(x_i) - \mathrm{E}_{c}(x_i)| / \sigma_{ч}(x_i) \cdot \sigma_{c}(x_i),$$

where $\mathrm{E}_c(x_i)$ is mathematical expectation (mean value) of the attribute values for a "Self" image, $\sigma_c(x_i)$ is root-mean-square deviation of attribute values for a "Self" image, $\mathrm{E}_ч(x_i)$ and $\sigma_ч(x_i)$ are the same parameters for a "Non-Self" image.

Attribute's handlers link with neurons of the first level step-by-step at first, and when the number of the neuron exceeds the number of attributes they link with neurons at random. The output of the summation function at the decision-making step is computed using the formula:

$$y = \sum_{i=1}^{m} \mu_i \cdot v_i + \mu_0 \tag{2}$$

where v_i is the i^{th} neuron input, m is a number of inputs, μ_i is a weight coefficient of the i^{th} input, μ_0 is a zero weight responsible for a neuron quantizer switch.

Despite of the perceptron, networks may be built of other functionals as well, Pearson metric, for instance (3). Pearson metric is a quadratic form [11] that does not take into account correlation links between attributes. That is why it demonstrates good results when it is used in combination with attributes that have low mutual correlation (less than 0.3).

$$y = \sum_{i=1}^{m} \frac{(E(v_i) - v_i)^2}{\sigma(v_i)^2} \tag{3}$$

where v_i is the i^{th} input of a neuron, $E(v_i)$ is mathematical expectation (mean value) of the i^{th} input of a neuron, $\sigma(v_i)$ is root-mean-square deviation of the i^{th} input of a neuron.

This paper considers a single-layer network based on Bayes-Pearson functional that computes an output using the formula (3). The computed value is compared with a threshold. Any neuron has its own best threshold that is selected in an empirical way based on the multiplication:

$$\theta = \chi_{max} \cdot a,$$

where χ_{max} is the maximum of a quadratic form when training samples of the "Self" image input, a is a stabilizing coefficient selected for any set of attributes experimentally. When the threshold is exceeded, the neuron outputs 1, in other way it outputs 0.

A computational experiment with biometric data was carried out. For any test person a neural network based on the functional (2) (the perceptron) and a neural network based on the functional (3) (a quadratic form network or Peason-Hamming network) were built. At least 21 samples from any test person were used to train the above mentioned networks, and 1 sample from 64 test persons was used to train the perceptrons (according to the requirements of GOST R 52633.5-2011). Other samples input the network for making decisions. A number of neurons and their inputs in this work is a parameter that varied in the process of the computational experiment. The results of the experiment are shown in Figures 5-7. Error probabilities were computed as a ratio of a number of false code outputs to a number of experiments carried out. By experiment we mean an attempt of generating a code based on user's authentic biometric data (data that belong to a certain user) or an attempt to forge a personal code using biometric data from another user (data input the network that corresponds to the user who owns the code to be generated). Errors were calculated for the cases of exact or partial key equality. In the first case the generated and the template code are treated as equal if the Hamming distance *Hd* between them is zero. In the second case a number of errors was counted when the Hamming distance was different ($Hd \geq 0$) between the generated key and the true key, then for any network configuration (a number of neurons and their inputs) the best Hamming distance was calculated that provides the least number of errors. The test validity was more than 0.99 when the confidence interval was 0.01.

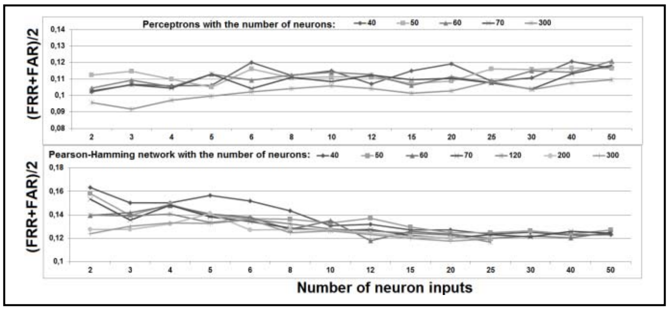

Fig. 5. Results of recognizing 100 persons in a set of basic attributes (the categories 1.1–1.2) when $Hd>0$.

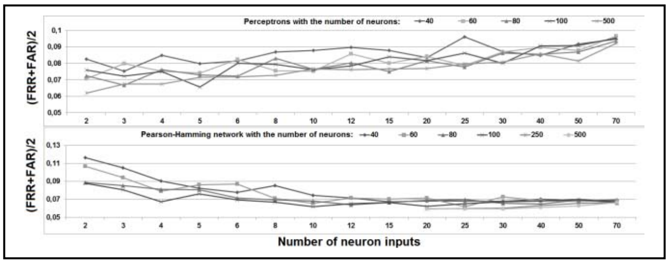

Fig. 6. Results of recognizing 100 persons in a set of basic and a part of supplementary attributes (the categories 1.1–2.2) when $Hd>0$.

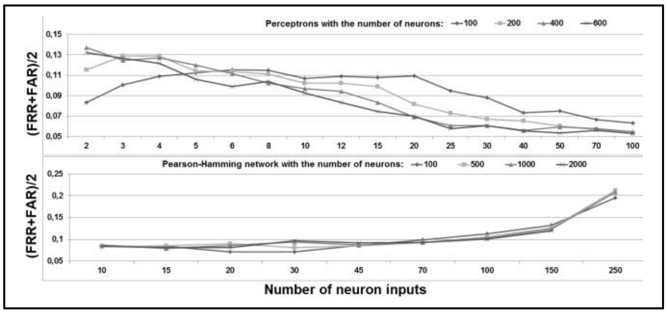

Fig. 7. Results of recognizing 100 persons in a set of all attributes (the categories 1.1-3.2) when $Hd>0$.

Analyzing the results of the experiments it may be noted that the dimension of the decision rule is worth increasing but not to the maximum possible level as an increase in a number of neuron inputs decreases error probability to a certain moment, after that moment the further increase in the functional dimension leads to a certain growth of an error level. An increase in a number of neurons does not deteriorate the situation, a number of neurons has to grow until their outputs are high correlated. In that case we manage to gain a significant advantage in the sum of probabilities for type I and type II errors. In particular, if users' images are verified without attributes that are obtained through Daubechies' wavelet transform (Fig. 5 and 6) is it better to increase a number of artificial neurons for the perceptron, and to enlarge the neuron dimension (a number of inputs) for Pearson-Hamming networks. The situation differs if we use attributes based on Daubechies' wavelet transform.

IV. Conclusion

Le us resume the main results:

1. A special keyboard is designed. The keyboard uses special sensors of pressure and vibration to record supplementary characteristics of keystroke dynamics.
2. A new category of attributes is proposed that is based on applying Daubechies' D6 wavelet transform to the function of pressure on keys and the function of keyboard vibration while typing a text. One password phrase consisting of 35 characters generates 720 attributes through the usage of the function of pressure and the function of vibration. It seems possible to obtain a larger number of low- and middle-correlated attributes (about 2000-3000, roughly estimated). The error probability will decrease, and the time required to process the operation of computing the attributes will significantly grow, however.
3. Laws of distribution for basic and supplementary attributes of keystroke dynamics are specified. It is established that the attributes based on the pressure on keys have the highest informative value
4. The estimation of correlation dependence for attributes was done: the dependence of basic (time characteristics of pressing keys) and supplementary attributes (key pressure and keyboard vibration) is low or negligible in more than 80% of cases. Thus, the proposed attributes contain new information about the user.
5. According to the results of the experiment (100 test persons) a number of errors while identifying 20 users were 0.6% if both basic and supplementary attributes were used. It is established that supplementary attributes may decrease twice or fourfold a number of errors (depending on a number of images to be identified).
6. In the verification mode the supplementary attributes allowed decreasing the error probability by 42.5%. The experiment demonstrated the following minimal probabilities for FRR and FAR while verifying test persons:
   - FRR=0.059, FAR=0.124 when basic attributes are processed by the perceptron network consisting of 300 neurons with 3 inputs trained according to GOST R 52633.5-2011.
   - FRR= 0,059, FAR=0,07 when basic attributes and a part of supplementary attributes (without wavelet coefficients) are processed by the Pearson-Hamming networks containing 250 neurons with 20 inputs.
   - FRR=0,047, FAR=0,058 when all attributes are processed by the perceptron network containing 600 neurons with 100 inputs trained according to GOST R 52633.5-2011.

According to the results of the experiments carried out the method of successive application of Bayes hypotheses formula demonstrates the best results in comparison with the single-layer perceptron and quadratic form networks. An approach that combines the above mentioned method of recognition seems to be rational. In general, the usage of supplementary attributes of keystroke dynamics for personal identification and verification is efficient.

References

[1] Global Data Leakage Report, H1 2016. InfoWatch. An access mode: [https://infowatch.com/sites/default/files/ report/InfoWatch_Global_Report_2016_ENG.pdf] (accessed: 12.03.2017).

[2] Center for Strategic and international Studies, Net Losses: Estimating the Global Cost of Cybercrime, June 2014, An access mode [https://csis–prod.s3.amazonaws.com/s3fs–public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf] (accessed: 13.04.2017).

[3] Moving forward with cybersecurity and privacy. An access mode: [http://www.pwc.ru/ru/riskassurance/ publications/assets/gsiss–report_2017_eng.pdf] (accessed: 21.05.2017).

[4] P.S. Lozhnikov, E. Buraya, A. Sulavko and A. Eremenko,"Methods of generating key sequences based on keystroke dynamics," Dynamics of Systems, Mechanisms and Machines (Dynamics*)* (Omsk), November 2016*,* pp. 1–5.

[5] P.H. Pisani, A.C. Lorena, "A systematic review on keystroke dynamics," Journal of the Brazilian Computer Society, 2013, vol. 19(4), pp. 573–587.

[6] Salil P. Banerjee, Damon L Woodard, "Biometric Authentication and Identification using Keystroke Dynamics: A Survey," Journal of Pattern Recognition Research, 2012, vol. 7, pp. 116–139.

[7] P.S. Lozhnikov, A.E. Sulavko, A.V. Eremenko, D.A. Volkov, "Methods of Generating Key Sequences based on Parameters of Handwritten Passwords and Signatures," Information, 2016, vol. 7(4), pp. 59.

[8] P.S. Lozhnikov, A.E. Sulavko, A.E. Samotuga, "Personal Identification and the Assessment of the Psychophysiological State While Writing a Signature," Information, 2015, vol .6, pp. 454–466.

[9] V.I. Vasilyev, A.E. Sulavko, A.V. Eremenko and S.S. Zhumazhanova, "Identification potential capacity of typical hardware for the purpose of hidden recognition of computer network users," Dynamics of Systems, Mechanisms and Machines (Dynamics) (Omsk), November 2016, pp. 1–5.

[10] A.I. Ivanov, E.I. Kachajkin, P.S. Lozhnikov, "A Complete Statistical Model of a Handwritten Signature as an Object of Biometric Identification," Control and Communications (SIBCON) (Moscow), May 2016, pp. 1–5.

[11] A.I. Ivanov, P.S. Lozhnikov, Yu.I. Serikova, "Reducing the Size of a Sample Sufficient for Learning Due to the Symmetrization of Correlation Relationships Between Biometric Data," Cybernetics and Systems Analysis, 2016, vol. 52(3), pp. 379–385.