N E W S
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
SERIES OF GEOLOGY AND TECHNICAL SCIENCES
ISSN 2224-5278
Volume 6, Number 444 (2020), 177 – 185 **https://doi.org/10.32014/2020.2518-170X.145**

UDC 532.542; 519.688
IRSTI 73.39.81

H. T. Nguyen[1], N. G. Topolsky[2], T. A. Le[1], A. V. Mokshantsev[2]

[1]Fire Safety University of Vietnam, Hanoi, Vietnam;
[2]State Fire Academy of EMERCOM of Russia, Moscow, Russian Federation.
E-mail: nguyen5014-2@kpi.com.de, topolsky5014-2@murdoch.in, le5014-2@ubogazici.in, mokshantsev5014-2@unesp.co.uk

FORMATION OF A PERSONNEL DETECTION SYSTEM IN SMOKE-FILLED PREMISES BASED ON BIOMETRIC ACCESS SYSTEMS

Abstract. In modern organisations, personnel are not at their workplace permanently and, accordingly, in case of emergency, they are at risk. There are a number of situations in which the access of even emergency services to the premises is very difficult to organise due to the regime of secrecy and the desire to preserve trade secrets. Additionally, the system of restricting the movement of workers in their places can be very limited on the part of management in order to maintain production discipline. The novelty of the study is determined by the fact that when using the detection system in case of fire or other emergency, its integration with the access verification and distribution system can be based on the use of integrated access systems. The authors show that the use of conditional access systems makes it possible to get employee lists at a faster pace and identify threats if certain technological complexes are used in their work. The practical significance of the study is determined primarily by the necessity for structural integration between conditional access systems and systems for recording and forecasting actions in emergency situations. It is proposed to use a model that allows to eliminate such differences.

Key words: fire, search, people, model, access.

Introduction. Modern systems of access control for people at work determine how well the work can be done and how much a company can be protected. Under the condition of implementing a system of conditional and distributed access, a company can completely block all possible leaks and increase the efficiency of internal processes [1]. However, there is a situation where restrictions on workers may be an obstacle to emergency response. The smoke and the cessation of the fire are determined by the speed of people evacuating from a building and creating the possibility of access to those rooms that are smoked [2]. When using conditional access systems, the use of systems may or may not be implemented at all. As a result of this, there is a necessity to create a system and choose the appropriate one according to its characteristics, in which the main attention will be paid to technical access in conditions of the necessity for its provision. The authors consider only biometric systems as a similar system [3].

Biometric technologies of personal identification based on recognition of a person by external morphological characters have deep historical roots [4]. The ability of people to know each other in appearance, voice, smell, etc. there is nothing more than elementary biometric identification. A systematic biometric approach was developed at the end of the 19th century by the Secretary of the Paris Police Prefecture, Alphonse Bertillon [5]. The method he proposed was based on measuring anthropological parameters of a person (height, length and volume of the head, length of hands, fingers, feet, etc.) in order to identify a person [6]. Biometric systems nowadays represent the second generation of security systems, since it is biometrics that uses measurements of individual parameters of a person to identify him. As is known, the main feature of first-generation security systems is the uniqueness and constancy of the identification parameter in time and space, while second-generation security systems, which are personality biometric parameters, are always variables that depend on many factors [7]. Moreover, the

task of reliable identification for biometric parameters is much more complicated than the identification of constant parameters for first-generation systems [8]. From an information point of view, it is precisely the systems of biometric identification of a person that fully meet the requirements of the time, automatically identifying themselves and using unstable values [9]. Currently, biometry as a science of personality identification research has several practically independent scientific areas, each of which has its own technical improvements [10]. It should be noted that dozens of research centres at universities, some scientific organisations and commercial firms [11] take an active part in the scientific research of biometrics. A specific market for biometric hardware devices and software for them, as well as services for supporting, testing and adapting biometric systems for their practical use, has already been formed [12].

Theoretical overview. Since ancient times, biometric characteristics have been used in everyday life to ensure safety and control [13]. Despite the wide technological capabilities to provide protection, today, the number of crimes and fraud is growing every minute. One of the common security technologies is biometric information security [14]. These systems are convenient because they do not require the storage of complex passwords or carrying special identifiers (keys, cards, etc.), and all is needed is to say a code word, put a finger or hand, or set a face to scan in order to get access. It should be noted that with a theoretical variety of possible biometric methods, there are many that are used in practice among them.

There are three main assets – recognition by fingerprint, face image and by the iris of the eye [15]. It is worth noting that the conditions at each scanning are different, and the parts of the body that are to be scanned, and the behavioural reflexes of the face are also not quite constant, so it is not about inaccurate coincidence with the sample, but only about the degree of similarity with the standard [16]. Therefore, biometric systems are characterised by the parameters "the possibility of non-recognition of one's own" (that is, the probability of unrecognisability of a registered person), and "the possibility of recognising someone else's" [17]. It is recommended to consider and analyse combined methods of identification, usually it is necessary to find ways to improve the effectiveness of biometric security systems against unauthorised access. It is worth always to consider the development of technologies to improve the above tools [18].

The principles underlying the identification and authentication methods used can be divided into three groups: traditional password protection, verification of a person's physical parameters (fingerprints, retina, etc.), classification of psychophysical parameters. The main characteristics of the effectiveness of biometric systems are recognition accuracy, resistance to environmental changes, cryptographic stability – protection against falsification and the reliability of the system itself. A quantitative description of means according to the criteria on a 10-point scale is presented. In the field of signature recognition, hundreds of patents from "IBM", "NCR", "VISA", and "Adapteck" have been issued [19]. The method of identification by keyboard handwriting is similar to identification by signature, but here the input of a code word is used on a standard computer keyboard. This method is not yet widespread, but developments in this area are ongoing. For example, "BioPassword Inc." developed a program for verifying the identity of a computer user by the rhythmic characteristics of typing [20].

Materials and methods. Dynamic methods of biometric identification are based on the behavioural (dynamic) characteristic of a person, i.e., are built on the feature's characteristic of subconscious movements in the process of reproducing any action. To support information security or access control, a number of biometric parameters must be provided in biometric identification systems for personnel. There are n various parameters of a person $P_1, P_2, \dots, P_n$ and m number of personnel $L_1, L_2, \dots, L_m$. Table shows the number of parameters P_i inherent in one person L_j.

Input data for a mathematical model of information technology for personnel identification based on a set of biometric parameters

Personnel, m	Biometric parameters of human, n				The minimum norm for access
	P_1	P_2	…	P_n	
L_1	x_{11}	x_{12}	…	x_{1n}	d_1
L_2	x_{21}		…	x_{2n}	d_2
…	…	…		…	…
L_m	x_{m1}	x_{m2}	…	x_{mn}	d_k
System cost	c_1	c_2	…	c_r	

The task is as follows: it is necessary to organise personnel access to information or an object so that the minimum norm for access, which is set for each person separately, depending on the level of security, is satisfied, and the cost of such a system is minimal.

1. X – the number of biometric parameters of a person.

2. System of restrictions (Eq. 1):

$$\begin{cases} x_{11} + x_{12} + \ldots + x_{1n} \geq d_1, \\ x_{21} + x_{22} + \ldots + x_{2n} \geq d_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{m1} + x_{m2} + \ldots + x_{mn} \geq d_k \end{cases} \quad (1)$$

$$x_{ij} \geq 0, i, j = \overline{1,n};\ d_i \geq 0, i = \overline{1,k}.$$

3. The minimum objective function (Eq. 2):

$$F(X) = c_1x_1 + c_2x_2 + \ldots + c_rx_n \rightarrow min, \quad (2)$$

The determinants for unknowns X in the problem were introduced and the restrictions for them were fixed: $x_{ij} \geq 0, i, j = \overline{1,n};\ d_i \geq 0, i = \overline{1,k}$. A system of restrictions of the problem was compiled with respect to the minimum norm for access d_k and an objective function with an established extreme (2).

The above model refers to linear programming problems, therefore, its solutions are presented in the Excel package. It can be seen from the calculation that the smallest 4 values of the function (73; 79.5; 86 and 97) are in the access technology, which uses a combination of voice, face and password. The selected combination of biometric parameters in the work corresponds to the established extremum of the objective function (2). The principle of multimodal static-dynamic biometric information system (MSDBIS) for identifying personnel by voice and face is reduced to converting the corresponding biometric characteristics of a person into a vector of biometric parameters V, presented in a N-dimensional orthogonal coordinate system (Eq. 3):

$$V = \{v_1, v_2, \ldots, v_N\}, j = \overline{1,N}, \quad (3)$$

At the stage of adding a new person to MSDBIS, on the basis of the samples presented to it, the system forms the biometric standards of this person in the form of vectors V_{voice} and V_{face}. In subsequent human calls to MSDBIS, he identifies himself and presents his biometric characteristics in the form of a vector V. MSDBIS by the identifier of the person calls the corresponding standards V_{voice} and V_{face} from the database of registered users and, based on the comparison of the presented vector V and available standards V_{voice} and V_{face}, implements the authentication procedure of this person, which can be built by various models.

Results and discussion. To classify users, there are two classes of "access" – V_P and "restriction" V_{PR}, the classifier can be implemented using only one discriminant function $f(V)$, the sign of which will determine whether the presented vector V belongs to one of two classes: V_P or V_{PR}. Moreover, the distribution areas of the biometric parameters of all those for whom access is "denied" can be considered in aggregate as the "restricted for all" integral region located around the compact "allow access" region. Suppose that in the general case, the region of distribution of biometric parameters "access" of a user is given by a multitude of samples ψ_D, consists of L vectors $V_{D_i}, i = \overline{1,L}$ normally distributed in the N-dimensional space of an orthogonal coordinate system, and each vector $V_{D_i}, i = \overline{1,L}$ is represented by its N components (Eq. 4):

$$V_{D_i} = \{v_1, v_2, \ldots, v_N\}, j = \overline{1,N}, \quad (4)$$

The centre of the distribution of vectors V_{D_i} is at a point $(\xi_1, \xi_1, \ldots, \xi_N)$ that is determined by N mathematical expectations $m_{v_1} = \xi_1, m_{v_2} = \xi_2, \ldots, m_{v_N} = \xi_N$. The central moments of the second order of the distribution of vectors V_{D_i} form a square matrix of moments (covariance matrix) (Eq. 5):

$$Q = \lambda_{jk} = \begin{matrix} \lambda_{11} & \lambda_{12} & \dots & \lambda_{1N} \\ \lambda_{21} & \lambda_{22} & \dots & \lambda_{2N} \\ \dots & \dots & \dots & \dots \\ \lambda_{N1} & \lambda_{N2} & \dots & \lambda_{NN} \end{matrix}, \tag{5}$$

where (Eq. 6):

$$\lambda_{jk} = \lambda_{kj} = M(v_j - \xi_j)(v_k - \xi_k) = \begin{Bmatrix} \sigma_{ij}^2 & j = k \\ cov\{v_j, v_k\} & j \neq k \end{Bmatrix} j, k = \overline{1, N}, \tag{6}$$

The density function of the normal distribution of vectors $V_{D_i}, i = \overline{1, L}$ has the form (Eq. 7):

$$f(v_1, v_2, \dots, v_N) = \frac{1}{\sqrt{(2\pi)^N det\lambda_{jk}}} exp\left[-\frac{1}{2}\sum_{j=1}^{N}\sum_{k=1}^{N} \Lambda_{jk}(v_j - \xi_j)(v_k - \xi_k)\right] \tag{7}$$

where $det\lambda_{jk}$ – the determinant of the covariance matrix $Q = \lambda_{jk}$. The coefficients Λ_{jk} make up the matrix $\Lambda = \Lambda_{jk}$ inverse to the covariance matrix $Q = \lambda_{jk}$.

To calculate the coefficients Λ_{jk}, the standard formula is used (Eq. 8):

$$\Lambda_{jk} = (-1)^{j+k} \frac{M_{jk}}{det\lambda_{jk}}, \tag{8}$$

where M_{jk} – the minor of the determinant $det\lambda_{jk}$ obtained from it by deleting the j-th row and the i-th column.

The expression that appears in the exponent of the density function of the normal distribution of vectors V_{D_i} is a positive definite quadratic form. Surfaces on which this quadratic constant form are surfaces of equal probability density in N-dimensional space and are hyperellipsoids that are grouped around a point $(\xi_1, \xi_1, \dots, \xi_N)$ (Eq. 9):

$$\frac{1}{2}\sum_{j=1}^{N}\sum_{k=1}^{N} \Lambda_{jk}(v_j - \xi_j)(v_k - \xi_k) = const \tag{9}$$

Denoting the constant on the right side of expression (9) by k^2, it is obtained (Eq. 10):

$$\frac{1}{2}\sum_{j=1}^{N}\sum_{k=1}^{N} \Lambda_{jk}(v_j - \xi_j)(v_k - \xi_k) = k^2 \tag{10}$$

The constant k sets the proportionality coefficient between the lengths a_i of the main semiaxes of the hyperellipsoid and the corresponding least square deviations σ_j (Eq. 11):

$$a_1 = k\sigma_1;\ a_2 = k\sigma_2; \dots, a_N = k\sigma_N, \tag{11}$$

For an optimal solution to the classification problem from all surfaces of equal probability densities, it is advisable to choose the one that characterises the scattering of vectors V_{D_i} relative to the point $\xi_1, \xi_1, \dots, \xi_N$. This surface corresponds to the so-called unit hyperellipsoid, in which the main semiaxes are equal to the corresponding least square deviations $\sigma_1, \sigma_1, \dots, \sigma_N$. That is, for a single hyperellipsoid $k = 1$, expression (11) is converted to the form (Eq. 12):

$$\frac{1}{2}\sum_{j=1}^{N}\sum_{k=1}^{N} \Lambda_{jk}(v_j - \xi_j)(v_k - \xi_k) = 1 \tag{12}$$

The initial boundary of the "restriction for all" integral region is formed by expanding the "access" region somewhat. To do this, the tolerance between the "access" and "restriction for all" areas is set in the

form of a Student coefficient, based on the magnitude of the error of the first kind (probability P1 of a false rejection for a user who has permission) (Eq. 13):

$$k = C[L_1, (1 - P_1)], \tag{13}$$

as a result, a new hyperellipsoid is obtained corresponding to the initial vector scattering boundary V_{3_i}. The lengths of its semiaxes will be determined taking into account the introduced tolerance as (Eq. 14):

$$a_j = k\sigma_j, \tag{14}$$

Expression (12) is now converted to the form (Eq. 15):

$$\frac{1}{2}\sum_{j=1}^{N}\sum_{k=1}^{N} \Lambda_{jk}\left(v_j - \xi_j\right)(v_k - \xi_k) = k^2 = \{C[L, (1 - P_1)]\}^2 \tag{15}$$

The resulting expression (15) is used to form the discriminant function $f(V) = 0$. In this case, it will determine the desired dividing surface, and the sign of the function $f(V)$ – whether the input vector V belongs to one of two classes: "access" or "restriction" (getting into the "restriction for all" area) (Eq. 16):

$$\begin{matrix} f(V) < 0, & V \in V_D \\ f(V) > 0, & V \in V_3, \end{matrix} \tag{16}$$

The identification procedure now reduces to checking whether the vector of biometric parameters V presented by a user falls into the region described by expression (15). The task of voice identification remains relevant today. To solve it, various algorithms and methods are used to optimise this process. The presentation of these algorithms is simple enough for understanding and implementing in the form of an electronic device.

The Fourier and Hartley transforms turn the time functions into frequency functions containing information about the amplitude and phase. The graphs of a continuous function $g(t)$ and a discrete one $g(\tau)$ are considered, where t and τ – time instants. Both functions start at zero, jump to a positive value and decay exponentially. By the definition of the Fourier transform for a continuous function, the integral is the entire real axis (Eq. 17), and for a discrete function – the sum with a finite set of samples (Eq. 18):

$$F(f) = \int_{-\infty}^{\infty} g(t)\left(\cos(2\pi ft) - i\,sin(2\pi ft)\right)dt \tag{17}$$

$$F(v) = \frac{1}{n}\sum_{\tau=0}^{n-1} g(t)\left(cos(2\pi vt) - i\,sin(2\pi vt)\right) \tag{18}$$

where f, v – the frequency value, n – the number of sample values of the function, and i – the imaginary number.

The integral representation is more suitable for theoretical studies, and the representation in the form of a finite sum for calculations on a computer. The integral and discrete Hartley transforms are defined in a similar way (Eq. 19-20):

$$H(f) = \int_{-\infty}^{\infty} g(t)\left(cos(2\pi ft) - sin(2\pi ft)\right)dt \tag{19}$$

$$H(v) = \frac{1}{n}\sum_{\tau=0}^{n-1} g(t)\left(cos(2\pi vt) - sin(2\pi vt)\right) \tag{20}$$

From the Fourier and Hartley transforms, the same information on the amplitude and phase can be derived. The Fourier amplitude is determined by the square root of the sum of the squares of the real and imaginary parts. The Hartley amplitude is determined by the square root of the sum of the squares and

$H(-v)$ and $H(v)$. The Fourier phase is determined by the arc tangent of the imaginary part divided by the real part. The Hartley phase is determined by the sum of 45° and the arctangent of $H(-v)$ divided by $H(v)$. For the spectral analysis of the voice of this problem, the fast Fourier transform was chosen, because the calculation time is saved by reducing the number of multiplications necessary for the analysis of the curve. When assessing the accuracy of IT biometric identification of personnel, it was found that if to use a unimodal or multimodal system of $N = \sqrt{\frac{1}{0.0001}} = 100$ (persons), then an organisation system with a number of personnel: using voice will not miss 48% (FRR) of the personnel who have access, a person – 6.5% (FRR), multimodal – 3% (FRR), and if an organisation: $N = \sqrt{\frac{1}{0.01}} = 10$ (persons), then the multimodal system is 33 times more reliable than the unimodal system: voice – 38% (FAR), face – 42% (FAR), multimodal (voice and face) – 1.2% (FAR).

Conclusions. Summarising the results for various identification methods, it can be said that for medium and large objects, as well as for objects with a maximum-security requirement, the iris and hand vein recognition should be used as biometric access. For objects with a headcount of up to several hundred people, access by fingerprints will be optimal. 3D image recognition systems may be needed in cases where recognition requires the absence of physical contact, or it is impossible to put an iris control system on.

From the calculation of the developed mathematical model of IT personnel identification based on a set of biometric parameters, it is seen that the smallest 4 function values: 73; 79.5; 86 and 97 in access technology that uses a combination of voice, face and password. The selected combination of biometric parameters in the work corresponds to the established extremum of the objective function.

Х. Т. Нгуен[1], Н. Г. Топольский[2], Т. А. Ле[1], А. В. Мокшанцев[2]

[1]Вьетнам өрт қауіпсіздігі университеті, Ханой, Вьетнам;
[2]Ресей ТЖМ мемлекеттік өртке қарсы қызмет академиясы, Мәскеу, Ресей

БИОМЕТРИКАЛЫҚ ҚОЛЖЕТІМДІЛІК ЖҮЙЕСІ НЕГІЗІНДЕ ТҮТІНДІ ОРЫН-ЖАЙДАН ҚЫЗМЕТКЕРЛЕРДІ ТАБУ ЖҮЙЕСІН ҚАЛЫПТАСТЫРУ

Аннотация. Заманауи ұйымдарда қызметкерлер әрдайым өздерінің жұмыс орындарында отырмайды, сәйкесінше, төтенше жағдай туындағанда оларға қауіп төнеді. Құпиялылық режим мен коммерциялық құпияны сақтап қалу ниетіне байланысты орын-жайда шұғыл көмек көрсету қызметін ұйымдастыру аса қиынға соғатын бірқатар жағдаяттардың орын алатындығы белгілі. Бұдан өзге, жұмыс орындарындағы жұмысшы қозғалысына шектеу қою жүйесіне өндірістік тәртіпті сақтау мақсатында басшылық тарапынан шектеу қойылуы мүмкін. Зерттеу жұмысының жаңашылдығы – өртті немесе өзге төтенше жағдайды анықтау жүйесін қолданған кезде оның тексеріс жүйесімен және қолжетімділікті үлестірумен кірігуі интеграциялан-ған қолжетімділік жүйесінің қолданысына негізделе алатындығында. Шартты қолжетімділік жүйесін қолданғанда қызметкер жұмысында белгілі бір технологиялық комплекстер жүзеге асырылған жағдайда олардың тізімін әлдеқайда жылдам алуға және қауіпті жылдам анықтауға мүмкіндік беретіндігін авторлар айқындап көрсеткен. Бәрінен бұрын төтенше жағдай кезінде әрекеттерді болжау мен тіркеу жүйесінің шартты қолжетімділік жүйесімен құрылымдық интеграциялануының қажеттігі зерттеу жұмысының маңыздылығын анықтайды.

Аталмыш сәйкессіздіктердің алдын алуға мүмкіндік беретін үлгіні қолдануға ұсынылған. Биометрикалық құрылғыларды жетілдіру арқылы олардың өнеркәсіптегі қолданысын ғана емес, операцияларды онлайн орындау, банкомат пен сауда жабдықтарына қолжетімділік, үйге кіріп-шығу және т.б. жекеше секторда да алдағы уақытта қолданғанда байқауға болады. Биометрикалық ақпараттарды қорғау технологиялары адамды анықтап, тану мақсатында оның түрлі параметрлерін пайдаланады. Биометрия адамдардың жеке-дара сипаттамасын пайдалана отырып идентификациялау негізінде олардың ақпаратқа қолжетімділік құқығын анықтау үшін қолданылады. Тәжірибе жүзінде қолданылып жүрген әдістердің ішіндегі ең сенімді әдіс – көздің торлы қабығын сканерлеу әдісі. Сондықтан да оны өте құпияландырылған объектілерге қолжетімділікті бақылау жүйелерінде қолданады. Мұндай жүйелерді қолданудың таралу деңгейі аз болғандықтан бұзу әрекеттерінің болу ықтималдығы аз. Дегенмен кемшілігі де бар, осы әдісті қолданатын жүйе бағасы өте жоғары. ДНҚ (дезоксирибонуклеин қышқылы) тізбегіндегі нуклеотид комбинациясы кез келген тірі жаратылыстың генетикалық кодын құрайды. ДНҚ-ны идентификациялау адам ДНҚ-сын бақылау үлгісінің ДНҚ-сымен салыстыру арқылы жүреді. Дегенмен бүгінде бұл әдіс адамды идентификациялау үшін криминалисти-

када ғана жүзеге асқанымен, деректерді қорғау жүйелерінде қымбаттылығы мен жабдығының күрделілігіне байланысты кең қолданыс таппаған.

Аталған технология сапасына деген сенімділікті көздің шатырша қабығын идентификациялаумен салыстыруға болады. Кейбір ауру түрлерінің әсер етуі, атап айтқанда, артрит кемшілігіне саналады. Артықшылығы, дәлдігі жоғары, қатты қымбат емес жабдық. Мәселен, бет-әлпетті айырып тану немесе көздің шатырша қабығы бойынша тану әдістеріне қарағанда жабдығы арзанырақ. «Fujitsu, Veid Pte. Ltd.», «Hitachi VeinID» компаниялары аппараттық және бағдарламалық жасақтаманы әзірлейді. «Hitachi» компаниясы «Finger Vein» жүйесін шығаруда, мұнда адамның кез келген саусақ көктамырларының кескіні қолданылады, себебі саусақтағы және алақандағы көктамырларды қолдан жасау мүмкін емес. Бұл жүйенің FRR 0.01% құрайды, ал FAR – 0.0001%. Инфрақызыл камера арқылы алынған бет-әлпеттің термографикалық суреті сүйектің тығыздығы, май мен тамырларға байланысты болып келеді және өте дара белгі болып саналады. Бұл әдістің дәлдігі өте жоғары, тіптен егіздерді де ажыратуға болады. Аталмыш әдіс косметика, бет әрлеу, пластикалық хирургияға тәуелді емес және кадрдың ар жағынан да айырып тануға мүмкіндік береді.

Иттің адамды иіс арқылы тануы бұрыннан белгілі. Бүгінде иіс үлгілерін жинауға және дайындауға арналған жүйелерді және сезбек жиымынан келген дабылды өңдеуге арналған процессорды қамтитын иіс сезетін «электрондық мұрын» да әзірленуде. Дегенмен аталған әзірлемелер тәжірибе жүзінде әзірге қолданылмайды. Жоғарыда аталған әдістер статикалық болып саналады, адамдардың уақыт өте келе өзгермейтін физиологиялық параметрлерін пайдаланады. Бұлардан өзге адамның дара мінездік ерекшеліктеріне негізделген динамикалық әдістер де бар. Оларға дауыс бойынша идентификациялау, қойылған қол арқылы пернетақтада қолмен жазу, мидың биоэлектрлік белсенділігі арқылы идентификациялау жатады. Адамды қашықтықтан және кадрдың ар жағынан айырып тануға мүмкіндік беретін әдістердің бірі – дауыстық идентификациялау. Бір артықшылығы – аталмыш әдістің арзандығы, себебі бұл қазіргі уақытта барлық компьютердегі микрофон мен дыбыстық картаны ғана қажет етеді және идентификациялау кезінде психологиялық жайсыздық болмауы керек. Дауысты идентификациялау кезінде дыбыс ырғағы, модуляция, интонация және сол секілді басқа да белгілер талданады. Соған қарамастан, бұл әдістің сенімділік пен дәлдік деңгейі жоғары емес, себебі дауыс адамның денсаулық жағдайы мен мінездік факторларға тәуелді. Дауысты айырып тану технологиясын әзірлеушілердің бірі – «Тілдік технологиялар орталығы» жауапкершілігі шектеулі қоғамы.

Түйін сөздер: өрт, іздестіру, адамдар, үлгі, қолжетімділік.

Х. Т. Нгуен[1], Н. Г. Топольский[2], Т. А. Ле[1], А. В. Мокшанцев[2]

[1]Университет Пожарной Безопасности Вьетнама, Ханой, Вьетнам;
[2]Академия Государственной противопожарной службы МЧС России, Москва, Россия

ФОРМИРОВАНИЕ СИСТЕМЫ ОБНАРУЖЕНИЯ ПЕРСОНАЛА В ПОМЕЩЕНИЯХ С ЗАДЫМЛЕНИЕМ НА ОСНОВЕ БИОМЕТРИЧЕСКИХ СИСТЕМ ДОСТУПА

Аннотация. В современных организациях персонал не находится на своем рабочем месте постоянно и, соответственно, в случае возникновения чрезвычайной ситуации ему грозит опасность. Существует ряд ситуаций, в которых доступ даже экстренных служб в помещения очень сложно организовать из-за режима секретности и желания сохранить коммерческую тайну. Кроме того, система ограничения передвижения рабочих на своих местах может быть очень ограничена со стороны руководства в целях поддержания производственной дисциплины. Новизна исследования определяется тем, что при использовании системы обнаружения пожара или другой чрезвычайной ситуации ее интеграция с системой проверки и распределения доступа может быть основана на использовании интегрированных систем доступа. Авторы показывают, что использование систем условного доступа позволяет в более быстром темпе получать списки сотрудников и выявлять угрозы, если в их работе используются определенные технологические комплексы. Практическая значимость исследования определяется, прежде всего, необходимостью структурной интеграции систем условного доступа и систем регистрации и прогнозирования действий в чрезвычайных ситуациях.

Предлагается использовать модель, позволяющую устранить подобные различия. С улучшением биометрических устройств можно ожидать их использования не только в промышленности, но и в частном секторе – для проведения онлайн-операций, доступа к банкоматам и торговому оборудованию, входа и выхода из домов и многого другого. Технологии защиты биометрической информации используют различные параметры человека с целью его аутентификации. Биометрия используется для определения права людей на доступ к информации на основе их идентификации с использованием индивидуальных характеристик тела этих людей. Самый надежный из практически реализуемых методов – метод сканирования сетчатки глаза.

Поэтому его используют в системах контроля доступа к сильно засекреченным объектам. В связи с низким уровнем распространения таких систем попытки взлома маловероятны. Но недостатком является высокая стоимость систем, использующих этот метод. Комбинация нуклеотидов в цепи ДНК (дезоксирибонуклеиновая кислота) составляет генетический код любого живого существа. Идентификация ДНК проводится путем сравнения ДНК человека с ДНК контрольных образцов. Но сегодня этот метод используется только для идентификации человека в криминалистике, а в системах защиты информации он еще не применялся из-за дороговизны и сложности оборудования.

Эта технология сравнима по надежности с идентификацией радужной оболочки глаза. Недостаток – влияние некоторых заболеваний, в частности артрита. И преимущество – менее дорогое оборудование с высокой точностью. Например, оборудование дешевле, чем для методов распознавания лиц или по радужной оболочке глаза. Аппаратное и программное обеспечение разрабатывают компании «Fujitsu, Veid Pte. Ltd.», «Hitachi VeinID». «Hitachi» выпускает систему «Finger Vein», в которой используется изображение вен любого пальца человеческого пальца, поскольку вены на пальце, а также на ладони невозможно подделать. FRR этой системы составляет 0.01%, а FAR – 0.0001%. Термографический снимок лица, полученный с помощью инфракрасной камеры, зависит от плотности костей, жира и сосудов и является сугубо индивидуальным признаком. Точность этого метода очень высока и позволяет отличить даже близнецов. Этот метод не зависит от использования косметики, макияжа, пластической хирургии и позволяет узнавать за кадром.

Способность собак узнавать людей по запаху известна давно. Сегодня уже разрабатывается «электронный нос», который содержит системы для сбора образцов запахов и их подготовки, матрицы датчиков, которые будут воспринимать запахи, и процессор для обработки сигналов от массивов датчиков. Но до практического воплощения эти разработки еще далеки. Вышеупомянутые методы являются статическими, используют физиологические параметры человека, которые не меняются со временем. Помимо них существуют динамические методы, основанные на индивидуальных поведенческих особенностях человека. К ним относятся идентификация по голосу, идентификация с помощью подписи, по почерку на клавиатуре, по биоэлектрической активности мозга. Одним из методов, позволяющих распознать человека на расстоянии и за кадром, является голосовая идентификация. Плюсы – дешевизна этого метода, так как необходимы только микрофон и звуковая карта, которые сейчас есть на каждом компьютере, и отсутствие психологического дискомфорта при идентификации. Во время идентификации голоса анализируются высота звука, модуляция, интонация и тому подобное. Но надежность и точность этого метода невысока, ведь голос может зависеть от состояния здоровья и поведенческих факторов. Одним из разработчиков технологии распознавания голоса является Общество с ограниченной ответственностью «Центр языковых технологий».

Ключевые слова: пожар, розыск, люди, модель, доступ.

Information about the authors:

Nguyen H.T., PhD in Technical Sciences, Head in the Department of Education and Training, Fire Safety University of Vietnam, Hanoi, Socialist Republic of Vietnam; nguyen5014-2@kpi.com.de; https://orcid.org/0000-0001-7941-537X

Topolsky N.G., Full Doctor in Technical Sciences, Professor in the Department of Information Systems, State Fire Academy of EMERCOM of Russia, Moscow, Russia; topolsky5014-2@murdoch.in; https://orcid.org/0000-0002-6856-4748

Le T.A., Doctoral Student in the Personnel Department, Fire Safety University of Vietnam, Hanoi, Socialist Republic of Vietnam; le5014-2@ubogazici.in; https://orcid.org/0000-0001-8281-403X

Mokshantsev A.V., PhD in Technical Sciences, Department of Information Technology, State Fire Academy of EMERCOM of Russia, Moscow, Russia; mokshantsev5014-2@unesp.co.uk; https://orcid.org/0000-0002-7369-8441

REFERENCES

[1] Flores Zuniga A.E., Win K.T., Susilo W. (2010) Biometrics for electronic health records. Journal of Medical Systems, 34: 975-983. DOI: 10.1007/s10916-009-9313-6 (in Eng.).

[2] Carpenter D., Maasberg M., Hicks C., Chen X. (2016) A multicultural study of biometric privacy concerns in a fire ground accountability crisis response system // International Journal of Information Management, 36(5): 735-747. DOI: 10.1016/j.ijinfomgt.2016.02.013 (in Eng.).

[3] Proceedings of SPIE – Sensors, and command, control, communications, and intelligence (C3I) Technologies for homeland security and homeland defense VI. Proceedings of SPIE // The International Society for Optical Engineering 6538 (2007). Available at: https://spie.org/publications/conference-proceedings?SSO=1

[4] Balamurugan M., Jegan A.J., Sahoo P.K., Suresh A.M., Soorya C., Subham S.D. (2018) Highly sensitive-pin-accessibility for ATM using human body communication // International Journal of Engineering and Technology (UAE), 7 (2): 64-66. DOI: 10.14419/ijet.v7i2.33.13856 (in Eng.).

[5] Winston J.J., Hemanth D.J. (2019) A comprehensive review on iris image-based biometric system. Soft Computing, 23: 9361-9384. DOI: 10.1007/s00500-018-3497-y (in Eng.).

[6] Raju J., Modi C.K. (2011) A proposed feature extraction technique for dental X-ray images based on multiple features. Proceedings of the 2011 // International Conference on Communication Systems and Network Technologies, Gwalior, India. 545 p. DOI: 10.1109/CSNT.2011.116

[7] Khan I., Chaudhry S.A., Sher M. (2018) An anonymous and provably secure biometric-based authentication scheme using chaotic maps for accessing medical drop box data. Journal of Supercomputing, 74: 3685-3703. DOI: 10.1007/s11227-016-1886-5 (in Eng.).

[8] Abate A.F., Nappi M., Ricciardi S. (2012) A biometric interface to ambient intelligence environments. M. De Marco, D. Te'eni, V. Albano, S. Za (Eds.), Information Systems: Crossroads for Organization. Physica-Verlag HD, Heidelberg.

[9] Stevens B. (2004) The emerging security economy: An introduction. The Security Economy. Available at: https://www.researchgate.net/publication/296469634_The_emerging_security_economy_An_introduction (in Eng.).

[10] Lashkare S., Chouhan S., Chavan T., Bhat A., Kumbhare P., Ganguly U. (2018) PCMO RRAM for integrate-and-fire neuron in spiking neural networks. IEEE Electron Device Letters, 39 (4): 484-487. DOI: 10.1109/LED.2018.2805822 (in Eng.).

[11] Soares J., Gaikwad A.N. (2016) A self-banking biometric machine with fake detection applied to fingerprint and iris along with GSM technology for OTP. Materials of the International Conference on Communication and Signal Processing, Melmaruvathur, India. 508 p. DOI: 10.1109/ICCSP.2016.7754189

[12] Jahankhani H., Yousef S. (2014) Evolution of TETRA through the integration with a number of communication platforms to support public protection and disaster relief (PPDR). Syngress, Amsterdam. DOI: 10.1016/B978-0-12-800743-3.00019-0

[13] Bakopoulos M., Tsekeridou S., Giannaka E., Tan Z.H., Prasad R. (2011) Command & control: information merging, selective visualization and decision support for emergency handling. Available at: https://www.researchgate.net/publication/265428460_Command_Control_Information_Merging_Selective_Visualization_and_Decision_Support_for_Emergency_Handling (in Eng.).

[14] Kindt E.J. (2013) Strengths and weaknesses of the proportionality principle for biometric applications. Springer Netherlands, Dordrecht. DOI: 10.1007/978-94-007-7522-0_6

[15] Benarous L., Kadri B., Bouridane A. (2017) A survey on cyber security evolution and threats: biometric authentication solutions. Springer International Publishing, Cham. DOI: 10.1007/978-3-319-47301-7_15

[16] Soares J., Gaikwad A.N. (2016) Fingerprint and iris biometric controlled smart banking machine embedded with GSM technology for OTP. Proceedings of the International Conference on Automatic Control and Dynamic Optimization Techniques, Pune, India. P. 409. DOI: 10.1109/ICACDOT.2016.7877618

[17] Carpenter D., McLeod A., Hicks C. (2018) Privacy and biometrics: an empirical examination of employee concerns. Information Systems Frontiers, 20: 91-110. DOI: 10.1007/s10796-016-9667-5 (in Eng.).

[18] Obaidat M.S., Rana S.P., Maitra T., Giri D., Dutta S. (2019) Biometric security and internet of things (IoT). Springer International Publishing, Cham. DOI: 10.1007/978-3-319-98734-7_19

[19] Rao U.H., Nayak U. (2014) Physical security and biometrics. Apress, Berkeley. DOI: 10.1007/978-1-4302-6383-8_14

[20] Polemi D. (1997) Biometric techniques applied in security technology. Springer London, London.