Proposals for the Application of Modern Biometric Methods and Systems for Carrying Out Control, Surveillance and Protection of Access to Data

Kryukova D.Yu.*
Department of Informatics and Mathematics
Vologda Institute of Law and Economics of the Federal Penitentiary Service of Russia, Vologda, Russia
magnyi@list.ru

Tesalovsky A.A.
Department of urban cadastre and geodesy
Vologda State University
Vologda, Russia
andrew-tesalovsky@yandex.ru

Mokretsov Yu.V.
Department of Administrative Disciplines
Vologda Institute of Law and Economics of the Federal Penitentiary Service of Russia, Vologda, Russia
warog@mail.ru

Anisimov N.V.
Department of urban cadastre and geodesy
Vologda State University
Vologda, Russia
nvanisimov1@gmail.com

Avdeev Yu.M.
Department of urban cadastre and geodesy
Vologda State University
Vologda, Russia
avdeevyur@yandex.ru

Lukashevich V.M.
Department of Technology and Organization of the Forest Complex
Petrozavodsk State University
Petrozavodsk, Russia
lvm-dov@mail.ru

***Abstract* — The article discusses the application of modern biometric methods and systems for identifying persons, exercising control and supervision of the special contingent in correctional facilities. A brief description is given of personality recognition methods, the problems and the need for their use in the penitentiary system of Russia are considered. The article discusses the biometric methods of identifying a person and the appropriateness of their implementation in the penal correction system, the use of an integrated approach in recognizing people in official activities, the problems of using biometric systems in institutions, and the task is to design a model for applying a biometric system in a particular institution. The article considers the need for the active implementation of biometric access control systems at checkpoints and at the premises, as well as the prevention of crimes in sensitive premises and on the perimeter, exists in absolutely all FSIN facilities. However, it is necessary to design models for the use of these tools in a particular institution, including process and functional ones, as well as carefully study all the advantages and disadvantages of each identification method, software and hardware product, in order to assess the possibilities of their implementation.**

Keywords — biometrics, biometric methods, biometric systems, biometric characteristics, identification, authentication, personality recognition, access control, control systems, information security, data access protection.

I. INTRODUCTION

Identification and tracking of the special contingent is one of the main problems in correctional facilities of the Federal Penitentiary Service of Russia, especially when they have to move to the industrial zone, as well as to civilian facilities located outside the institution. Penitentiary staff should be as vigilant as possible during the escort of convicts and at crossing checkpoints. Due to downsizing of security personnel of institutions, timely detection of escape attempts on the perimeter of the institution, as well as the identification of the person trying to commit it, also plays a special role. Despite the decrease in the number of prisoners in institutions in recent years, quite often violations of the regime established inside the facility are recorded, which determines the urgent need for early identification of instigators, accomplices and others in order to prove their guilt. Many violators and their relatives (or accomplices) use modern and increasingly technically sophisticated methods of organizing crimes both within the institution and beyond.

The old methods of identifying employees and convicts, such as official identification cards, photographing, and conducting paper personal files, often themselves become an instrument of forgery, falsification, and fraud. Tracking visitors is another major problem in the facility. Visitors can not only create threats to information security, but also impose an additional burden of control on employees. Visitors try to bring weapons, mobile phones, drugs to the convicts, which is an illegal act and can lead to illegal actions, as well as to unrest in the institution. In addition to the above, visitors can create a threat during a meeting regarding the transport of technical equipment that allows connecting to the institution's local network, which is fraught with malfunctions in its work, data theft, their use and modification for criminal purposes. Many researchers agree that traditional methods of personality recognition require at least adjustment, and in some cases, abandonment. In connection with the foregoing, the application of modern biometric methods for identifying a person within the FSIN institution is relevant. Thus, we set the task: to consider the types of biometric identification of a person and the appropriateness of their implementation in the penal system, the use of an integrated approach in recognition, proposals for designing a model for the application of the system of biometric means in institutions.

II. LITERATURE REVIEW AND METHODOLOGY

The biometric method of personal identification is a method of statistical measurement of the physiological and behavioral characteristics of a person, which can be used to uniquely identify a person using biometric applications, such as recognition of fingerprints, images of the iris of the eye, analysis of DNA polymorphism, etc. Biometric features are divided into physiological and behavioral, where physiological biometry includes fingerprints, an eye iris or retina pattern, face geometry, finger or palm vein drawing, DNA polymorphism, oral dental matrix, facial thermogram, heart rate. Behavioral characteristics of a person include voice, rhythm of movement and gait, handwriting, and features of working on a computer keyboard.

Traditional identification and authentication systems include methods based on either ownership or knowledge. A person holding an identity card, driver's license or passport can use them to verify their identity. This method creates the risk of duplication, theft or loss of the document. A knowledge-based security system includes passwords, PIN codes, and codes. This method also has disadvantages, such as risks of losing or compromising passwords. Biometrics, however, has the ability to address these shortcomings and can serve as an identification system that cannot be forgotten, stolen, transmitted or duplicated.

A number of biometric characteristics associated with a person's personal data, such as name, date of birth, age, address, phone number, can serve as a way to identify or authenticate all employees of the institution, incoming and released convicts, visitors and provide almost perfect protection of classified information. Once this association is established, biometrics can be used for lifelong identification of a person. The biometric identification method is safer, faster and more reliable than knowledge and ownership-based identification methods.

It is necessary to make a reservation that as a result of age-related changes, illness or other circumstances, a person's voice, retina, geometry of a hand may change, fingerprints may disappear. However, with the rapid development, active study and widespread use in practice of biometric methods, weaknesses and limits of applicability of specific methods are identified, their shortcomings are eliminated, new technical solutions and software appear and improve. For example, multispectral scanners read information about the subsurface layer of the skin of a finger, which prevents the possibility of using a dummy of a finger or its fingerprint.

All methods of biometric identification of a person work according to the basic principle of comparing an existing data template and a biometric template with a new sample to either confirm who they call themselves or find out who they are.

There are many human biometric parameters that can be used as a basis for identification. Next, we consider the basic methods of biometric personality identification, used everywhere in the modern world, and the possibility of their use in the penal system.

1) Fingerprint Recognition

Fingerprint biometric analysis is considered the cheapest, most used and easiest to use identification method. Identification of a person is also easier with a fingerprint scan compared to other methods. In this identification method, a person's finger (one or more) is scanned and unique points are determined. This scanned data passes through a biometric system that contains predefined standard algorithms for generating unique template data. After creating the template data, the image of the scanned finger is deleted, and the template data is saved in the database. When a person needs to be identified again, the fingerprints are re-scanned again, and the system tries to match the scan to what has already been saved. If it matches, the person is identified.

The time taken to identify a person using a biometric system using a fingerprint in an ideal situation is less than one second.

In penitentiary institutions, for monitoring and supervising convicts and persons under investigation, biometric identification systems are also used—stationary and portable fingerprint readers, fingerprint records are being kept.

2) Face recognition

The face recognition system can identify people by processing their digital images, if their face identification has been previously carried out. Digital images or frames from a video source are used, which are shot using the face recognition algorithm. The algorithm extracts data from facial characteristics, such as the position and shape of the eyes, nose, cheekbones, and jaw. It can also measure the distance between these characteristics, and the displayed data is stored in the database.

The system can be useful for identifying convicts in a crowd, for example, during a mass exit to work, in an

industrial zone, in a dining room, in dedicated corridors between a residential and industrial zone. The face recognition system can capture several images per second, compare them and get results.

When recognizing by the geometry of the face, a three-dimensional model is built, and the pattern of a certain person takes into account many variations of the image for cases of face rotation, tilt, changes in lighting, facial expressions. Some algorithms allow compensating the presence of glasses, hats, mustaches and beards.

An important factor in the development of this direction is the widespread use of video surveillance in prisons (video cameras, video recorders, tablets).

3) Iris recognition

Iris recognition is a method of biometric identification based on the uniqueness of the patterns of the iris of each person. These unique samples are mathematically compared and stored by a recognition system, and can be used to establish a person's identity. The iris is the colored part that forms a ring around the central circular part of the eye. The iris is considered an ideal part of the human body for biometric identification, since, being an internal organ, it is protected from damage, unlike fingerprints, which can be intentionally or accidentally damaged. The iris of the eye remains protected behind a transparent cornea and is easily visible from a distance. The iris recognition system captures the image of the eye and starts the recognition algorithm with its help, as a result of which the unique template data is stored in the database and can be associated with human personality data.

4) Recognition of finger veins, palm veins

This biometric identification method recognizes the pattern formed by the veins in the human finger under the skin surface. The vein pattern is fixed by a special installation, which uses a near infrared LED and a monochrome camera. LEDs absorb hemoglobin in the blood and cause veins to appear as dark lines. The camera captures the image, and the identification system extracts a pattern of veins on the fingers. This sample is mathematically displayed in the system and can be used to identify a person, the same procedure is repeated to verify the identity.

This method is non-contact, provides a high level of security (the system requires blood flow in the veins to capture an image), but requires cumbersome expensive equipment, which so far prevents its widespread use, including in prisons.

5) Voice biometrics

Voice biometry is a method of identifying a speaker with a sample and matching his voice patterns. The voice, being a unique behavioral characteristic of a person, can be used to establish personality. Voice sampling is a fairly simple procedure and is usually performed using high-quality recorders. A voice sample is taken using a recognition algorithm to match the pattern. Once a pattern is matched, it can be associated with a person's personality. The technology of voice biometrics can be used to wiretap telephone conversations of convicts and persons under investigation.

6) Hand geometry

Each person has an individual hand shape. The hand geometry method for identifying a person can be used to monitor prisoners' visits to various places within the institution, access control, etc. The reader is used to measure hands in various projections, this data is stored. The biometric geometry of the hand is not considered as accurate as other methods (for example, fingerprint or iris recognition), due to the possibility of changes (trauma, illness, aging) of the shape of the hand, joints, skin during a person's life. However, recognition of a subject by hand geometry can be combined with pattern recognition of veins on a single device.

7) DNA biometrics

Despite the similarity of 99.9 % of the DNA sequence, a difference of 0.1 % is sufficient to identify a person. DNA biometry is significantly different from other standard biometrics, which are based on the impression, image or recording of physiological or behavioral characteristics. Identification by DNA profiling requires a physical sample of human tissue. The identification process is not as fast as other biometric methods, but it gives very reliable results, and there is no likelihood of false positives. The sample can be collected by non-invasive or invasive methods, for example: a buccal swab (collecting cells from the inside of the cheek), blood, saliva, sperm, or vaginal lubrication. Samples are taken using one of the various DNA analysis methods, and an electronic DNA profile is created in the database. These results are compared with other samples to find a match. DNA registration is invaluable in preventing or solving crimes.

The quality of biometric systems is characterized by the following indicators:

- FRR false failure rate – the probability of a failure to identify a user in the database;
- FAR false pass coefficient – the probability of false identification of a user who is not in the database;
- as well as resistance to counterfeiting, the environment, ease of use, speed, cost, etc.

Let us evaluate biometric methods from another point of view – as the most actively developing in recent years. A review of the main trends in the development of the biometric industry in 2018 [2] showed the presence of three leading areas: face recognition, fingerprints and multimodal technologies (a combination of recognition methods by face, iris, fingerprints and voice). The most promising and preferred approach, especially in inspection systems, experts call multimodal.

Based on a table of qualitative characteristics and an overview of prospects and development trends, from the point of view of application in penal correction systems, identification (authentication) by fingerprints, hand geometry, vein pattern (if possible combining on one device) is of greatest interest, non-contact methods by face geometry, gait (to identify a person from the crowd, when moving a group, at a remote distance), as well as DNA to prevent crimes or solve

them. It is interesting to consider combinations of some methods as part of a multimodal approach.

III. RESULTS

In order to provide maximum protection against unlawful access by unauthorized persons from outside, against illegal actions and escapes of convicts inside the institution, it is necessary to establish and ensure uninterrupted operation of the recognition system. It must be considered as a complex of at least 2–3 methods of biometric identification for solving various service tasks. This system should function along with and in parallel with integrated security systems, access control and control systems, and others.

At the moment, when speaking about the application of biometric methods in penal correction systems, they mean, first of all, biometric identification systems—recognition and accounting systems in rooms (for example, in canteens), at workplaces, etc. But there is also biometric authentication and almost always associated authorization. After checking the authenticity of the claimed user (authentication) the procedure for granting him certain authority and resources in the system (authorization) follows. From the point of view of control and supervision of convicts and persons under investigation, the administrative procedure is important—registration of user actions in the system, including their attempts to access resources.

Consider some areas of performance that require an integrated approach to identify individuals and protect sensitive information:

- application of a combination of methods for identification, authentication, authorization and administration of actions of employees and special contingent;
- application of methods of identification at the checkpoint for the admission of people (preferably the most accurate: by fingerprint, retina, finger veins);
- protection of the perimeter of the institution, especially "blind" sites and transitions "residential zone – industrial zone" identification systems, including video capture and face recognition;
- protection of access to special rooms, server rooms based on voice biometrics, and even better—by retina, face recognition, palm vein or using multimodal methods;
- creation of a database for recognizing visitors, based in the simplest case on fingerprinting, in more complex ones on the system of facial recognition, retinal identification, multimodal methods, and by DNA for relatives;
- application of voice biometrics to monitor telephone calls of convicts and investigate criminal offenses in the FSIN;
- application of the hand geometry recognition method to control access to a correctional facility for such persons as public figures, lawyers, legal representatives of convicts and persons under investigation (its drawback is low accuracy);
- application of the latest unmanned aerial vehicles (drones) with a built-in system for identifying and video recording persons on the territory of the institution, on the perimeter, in the industrial zone and on site using the labor of convicts;
- application of portable and stationary biometric systems (with recognition of fingerprints, in the more expensive version with the recognitions of the iris) at remote sites, for example, in civilian enterprises where convicted labor is used;
- comprehensive data collection of convicts upon their admission to the institution and step-by-step identification using biometrics upon release;
- application of DNA biometrics to investigate criminal offenses committed inside and outside the institution;
- legalization of methods of post-penitentiary control of released persons using banks of various biometric data;
- implementation of aspects of the concept of "smart colony" using biometric systems for identification and data protection [3]. The provision of resources and services in the institution of penal correction system can be carried out using bio-identification technologies: accounting for working hours and procedures for obtaining and handing over a special tool, labor results; registration, control and supervision of movements during the day; requests to the library, to the medical unit; admission to various places, on dates, appeals to management.

Today, many correctional facilities and pre-trial detention centers of the Federal Penitentiary Service of Russia already successfully operate software systems with biometric components as part of control systems and access control for people at checkpoints, access control to special accounting data [4]. Basically, they incorporate the principles of face recognition and fingerprinting. Examples of such hardware and software systems include:

- "Synerget SKDL", issued by Stilsoft [5] (the principle of identification by fingerprints and face);
- Software package "Automated accounting of the special contingent"; the developer is the Research Institute of the Federal Penitentiary Service of Russia, Tver (access by fingerprints is possible) [6];
- ACS "Biosmart" by engineering company "Prosoft-Biometrix" (fingerprints and palm vein of the palm);
- Papilon automated fingerprint information system (ADIS), JSC Papilon (fingerprints).

Modern biometric systems allow creating multibiometric data banks of any volume and various target orientations. For example, in ADIS Papilon [7], in addition to fingerprints and palms, it is possible to store two- and three-dimensional images of the person, the iris, handwriting samples, DNA

descriptions, etc. It is possible to quickly verify the identity using peripheral stations.

Undoubtedly, the application of the above biometric methods is necessary when organizing access, security and regime in the institutions of the Federal Penitentiary Service. However, the use of software and hardware systems with biometric components in institutions has a number of problems:

- high price;
- obsoleteness of computer networks and systems within a number of institutions to install such systems, the absence or obsolescence of server equipment;
- rather "immature" software for such systems on the Russian market. This implies either dependence on a foreign software manufacturer, or weak and unsystematic technical support and updating of Russian programs;
- lack of legislation allowing the full legitimacy of the use of complex identification systems of any person without his written consent (conflicts with the law on the protection of personal data [8]);
- need for mandatory warning of persons about the use of control and bio-identification systems allows violators to be mentally and physically prepared, to come up with the possibility of cheating systems;
- need for lengthy testing of new systems in the conditions of various types of FSIN institutions in Russia;
- weak point of biometric systems is the possibility of using dummies.

IV. CONCLUSION

In conclusion, we note that the need for the active implementation of biometric access control systems at checkpoints and premises, as well as the prevention of crimes in sensitive premises and on the perimeter, exists in absolutely all FSIN facilities [9]. However, it is necessary to design models for the use of these tools in a particular institution, including process and functional ones, as well as carefully study all the advantages and disadvantages of each identification method, software and hardware product, in order to assess the possibilities of their implementation.

Thus, the article discusses the biometric methods of identifying a person and the appropriateness of their implementation in the penal correction system, the use of an integrated approach in recognizing people in official activities, the problems of using biometric systems in institutions, and the task is to design a model for using the biometric system in a particular institution.

References

[1] Biometrics from "A" to "Z" a complete guide to biometric identification and authentication. Retrieved from: https://securityrussia.com/blog/biometriya.html (accessed: 03/07/2019).

[2] Russian biometric portal BIOMETRICS.RU Retrieved from: http://www.biometrics.ru/ (date of access: 03/07/2019).

[3] Yu.V. Mokretsov, D.Yu., Kryukova, Institutionalization of the concept of "smart colony" in the penal system of Russia", Information and technical support for the activities of territorial bodies and educational organizations of the Federal Penitentiary Service of Russia, Coll. Mater. scientific-practical a workshop. Vologda: VIPE Federal Penitentiary Service of Russia, 2018, pp. 61–68.

[4] "Biometric identification: fake is not possible", Prison J. Crime and Punishment, no. 12, pp. 18–20, 2018. URN FSIN of Russia.

[5] SPO Synerget SKDL. Official website of the Steel Soft company. Retrieved from: http://www.stilsoft.ru/catalog/sinerget-skdl (accessed: 03/07/2019).

[6] D.Yu. Kryukova, O.A. Panfilova, "Problems of ensuring information security in the software package for automated filing records of a special contingent", Bull. of the Voronezh Instit. of the Fed. Penitentiary Service of Russ., no. 3, pp. 104–109, 2018.

[7] Papillon Systems. official site of Papillon JSC. Retrieved from: http://www.papillon.ru/rus (date of access: 03/07/2019).

[8] D.Yu. Kryukova, Yu.V. Mokretsov, "Actual problems of legal regulation of turnover and protection of personal data in Russia", Institute Herald: crime, punishment, correction, vol. 2, no. 38, pp. 34–38, 2017.

[9] D.Yu. Kryukova, A.A. Babkin, Information support of the penal system: problems of organization and improvement. Vologda: VIPE FSIN of Russia, 2018, 106 p.