

Alternative biometric, as method of information security of healthcare systems

Andreeva Ekaterina

Saint-Petersburg

*State University of Aerospace Instrumentation,
Department of Information Security Technologies*



Outline



Problems of information security in healthcare systems



Why alternative methods of biometrics should be used?



Two ways of application biometric technology using heart sounds for information security

Topicality

- Every year appear more and more medical devices for diagnosis of human condition
- Medical human personal data has high level of privacy
- Medical information is protected using standards of information security



Access control

Data encryption

Features of information security systems for medical devices



Information security system should not depend on the user activity



Information security system should not depend on the user condition



Information security system should be reliable and attack-resistant

Comparison between biometric traits



Password

- Simplicity to use
- Required active input data, possibility of loss or theft



Fingerprint

- High accuracy of authentication, reliability.
- Biometric feature may be lost or damaged, required active input data



DNA

- High accuracy of authentication, non-obligatory procedure of input data
- Complex analysis procedure, complex procedure of input data



Voice

- Simplicity in data accumulation, possibility of substitution
- Possibility of loss or theft, required active input data

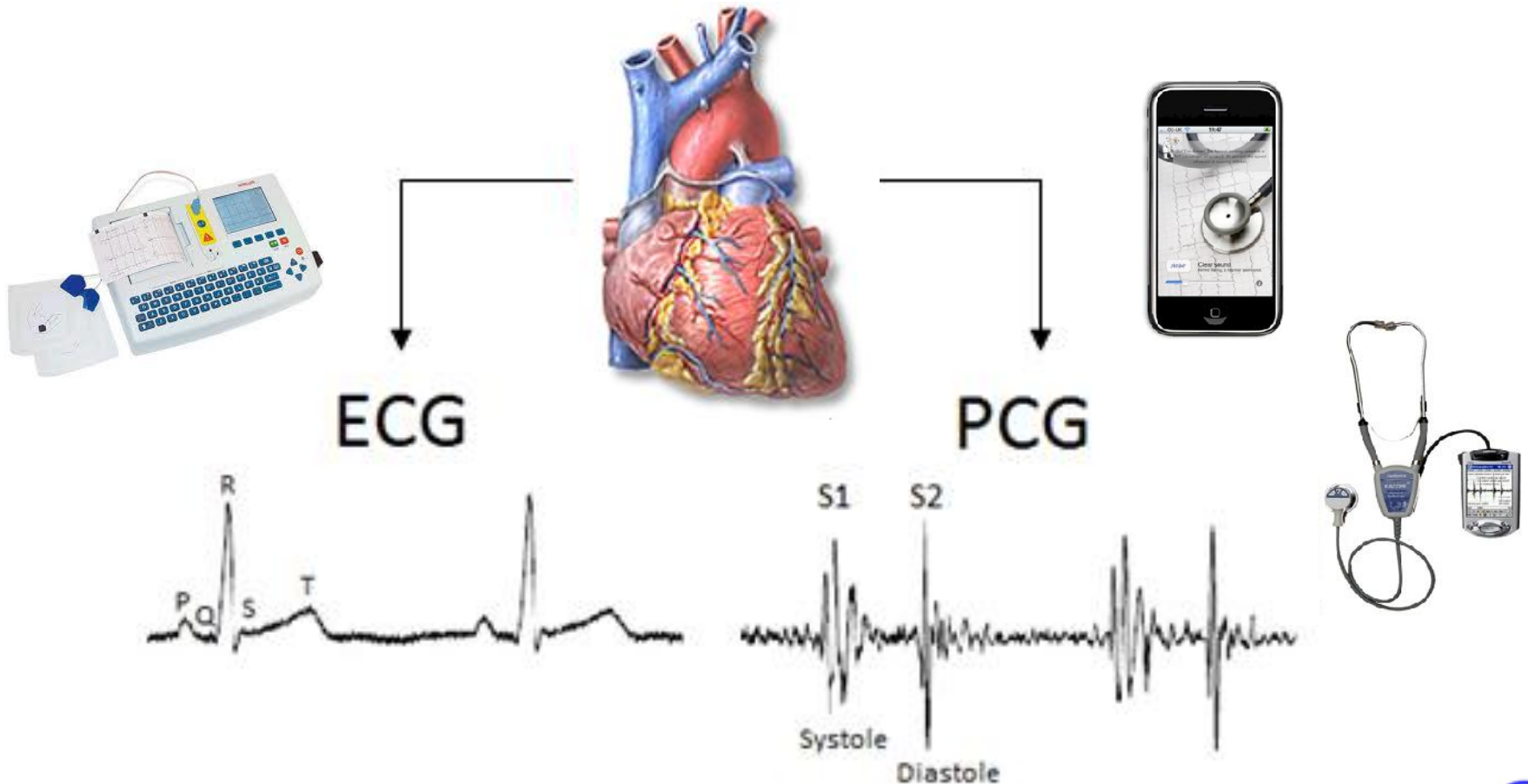


Heart sounds

- Simplicity to use, non-obligatory procedure of input data
- Complex analysis procedure

Biometric recognition using heart sounds

The heart is involved in the production of two biological signals



Biometric recognition using heart sounds

- Heart signals can not be lost during the life
- Heart signals are difficult to be falsified
- Access control may be performed without any user actions and continuously during operation of medical devices
- Heart signals allow to diagnose the person physical and psychological condition



Two ways of application biometric technology using heart sounds in information security systems



Authentication

- Database
- Features
- Classification

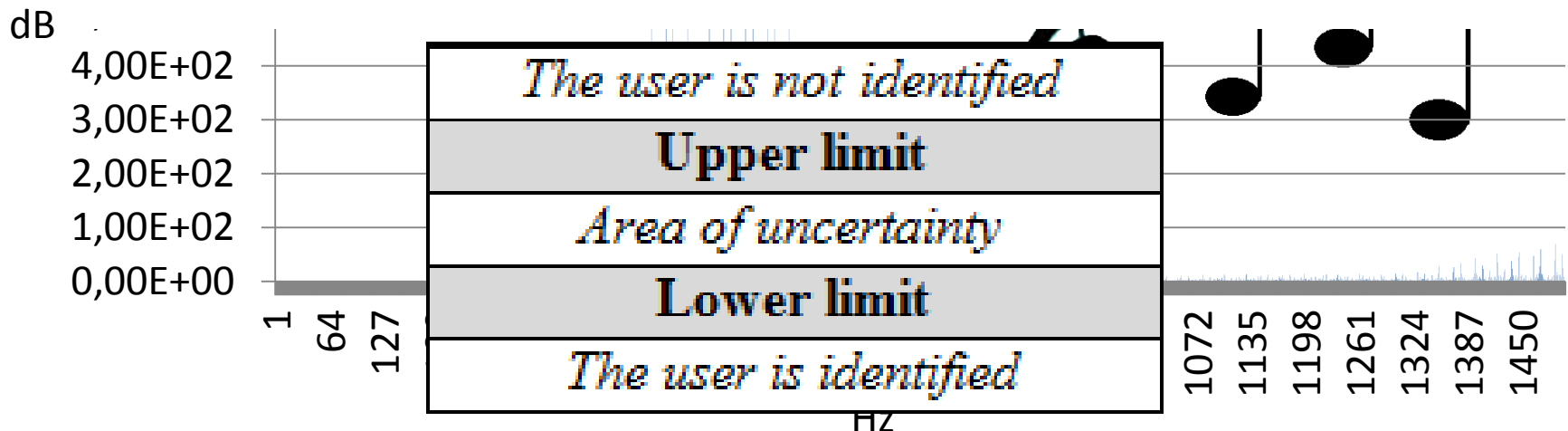
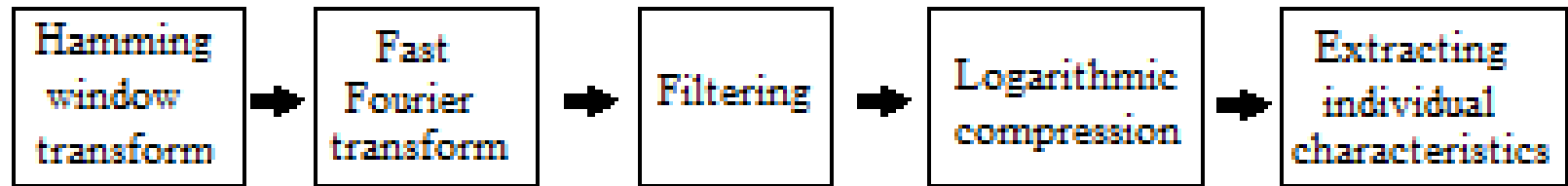


Secure data transmission

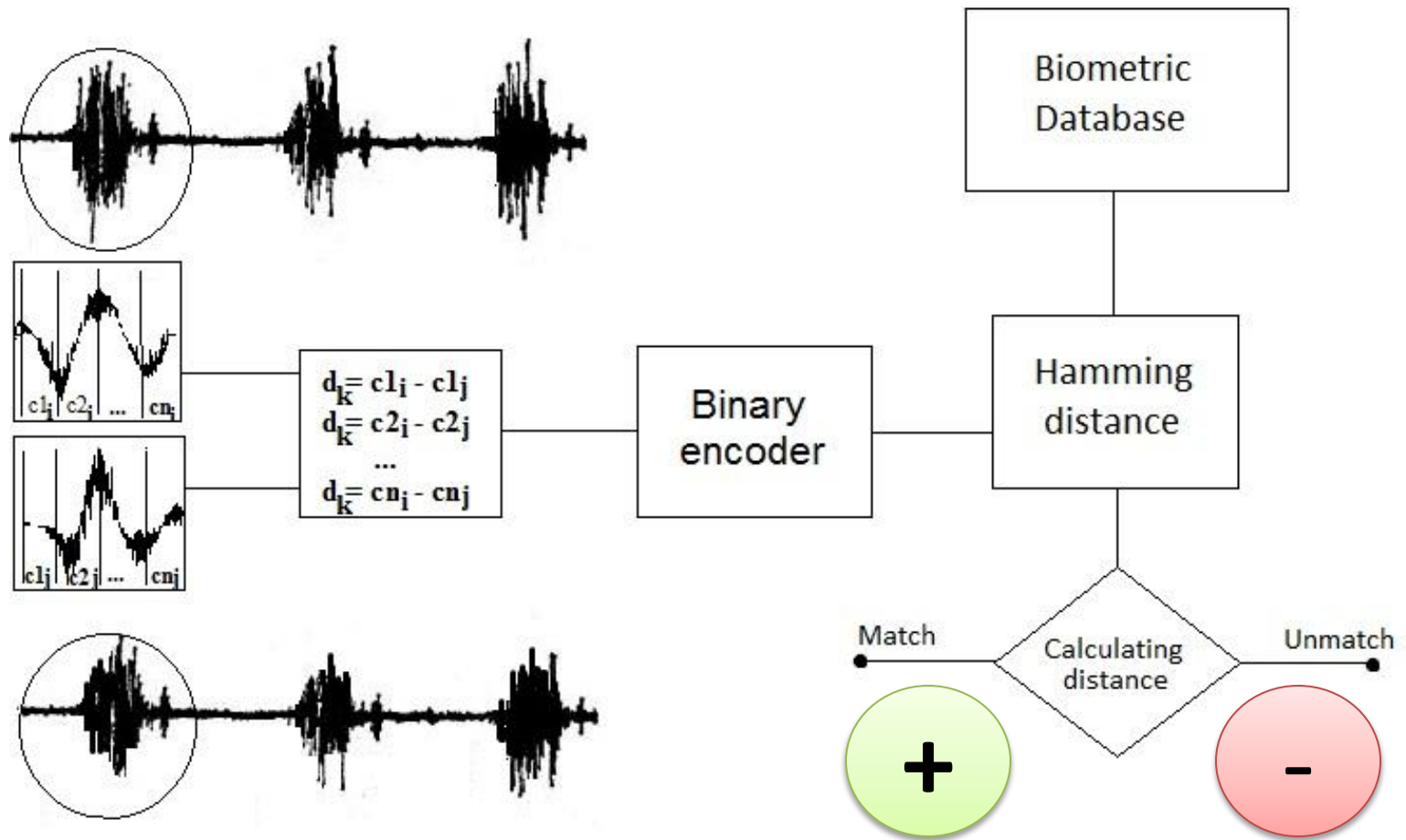
- Key generation
- Encryption
- Decryption

Authentication solution

- The use of heart sounds signals as the authentication method is possible due to availability of a melody which is typical of every specific man



Authentication solution

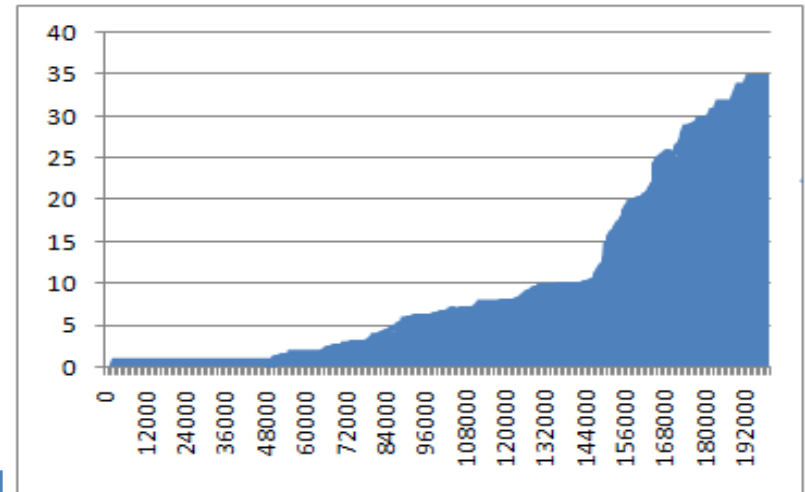


Binary encoder

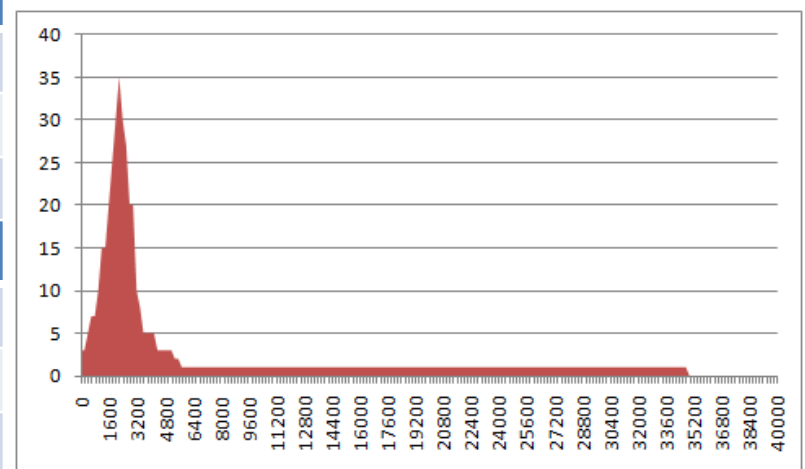
- Upper limit = 70000
- Lower limit = 5000

$$v_i^A = \begin{cases} 1, & \text{if } w_l > MAX \\ 0, & \text{if } w_l < MAX \end{cases}$$

$$v_i^B = \begin{cases} 1, & \text{if } w_l > MIN \\ 0, & \text{if } w_l < MIN \end{cases}$$



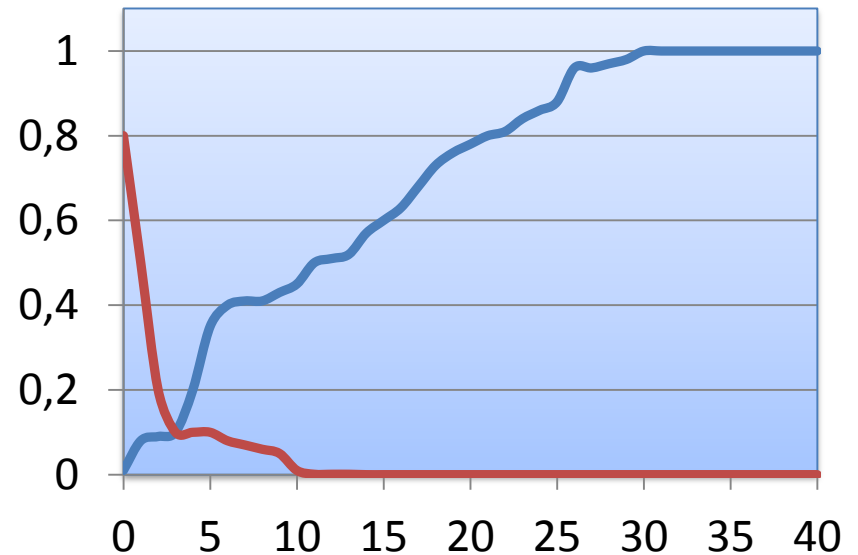
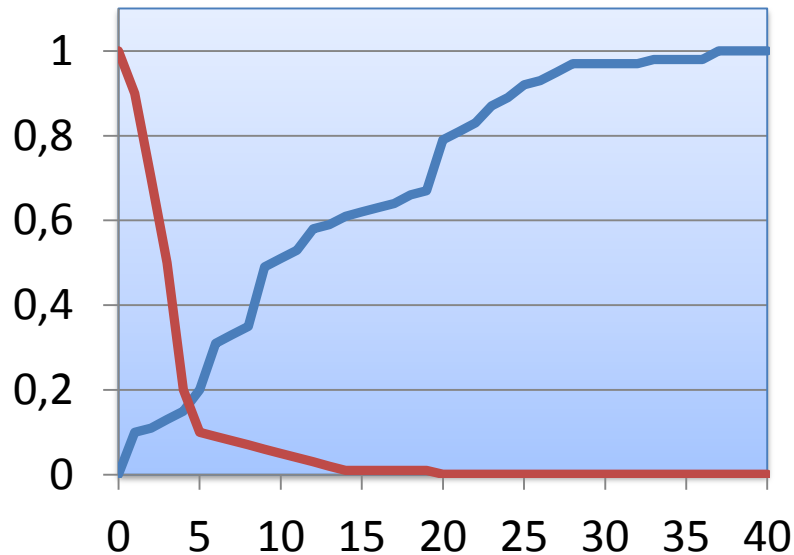
	v1	v2	v3	v4	v5	v6	...	v40	W
S1	1	0	0	1	1	1	...	0	15
S2	0	0	0	0	0	0	...	0	0
S3	0	0	0	0	0	1	...	0	3
	v1	v2	v3	v4	v5	v6	...	v40	W
S1	1	1	1	1	1	1	...	1	40
S2	0	0	0	0	1	0	...	0	1
S3	1	1	1	1	0	0	...	1	26



Analysis of results

— FAR
— FRR

Selected parameters can achieve a compromise between system performance and minimize errors in the system

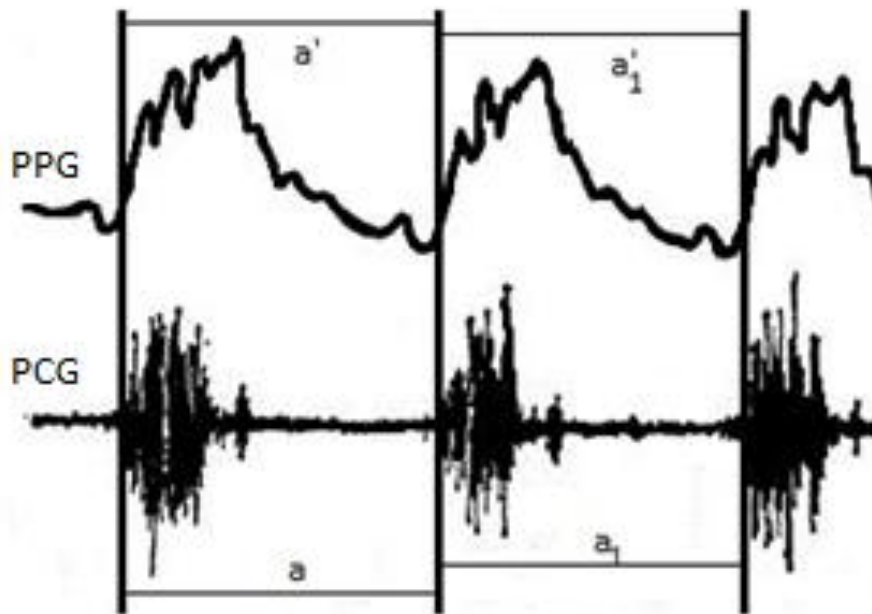


FAR - false accept rate

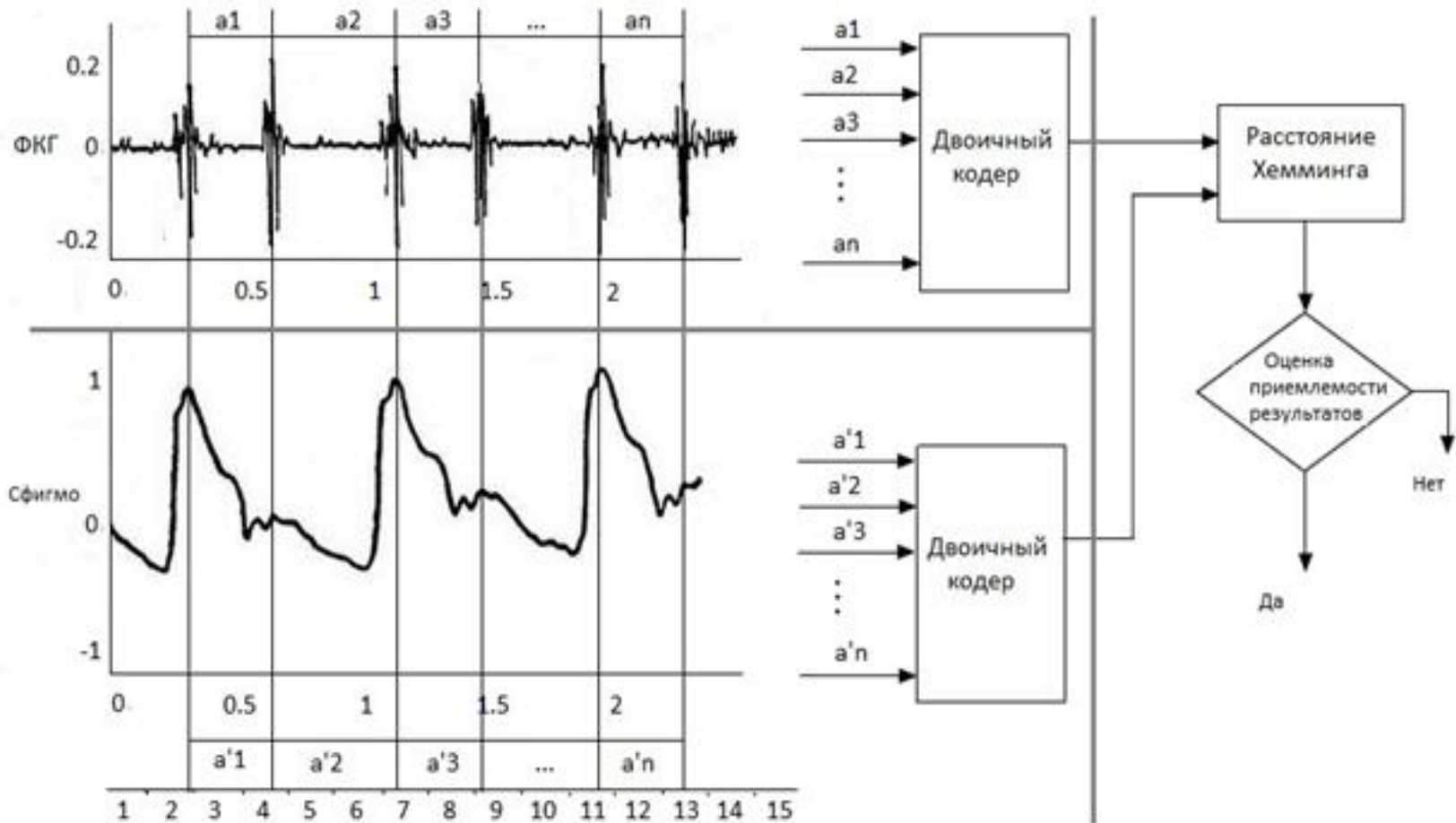
FRR - false reject rate

Solution for secure data transmission

- For secured distribution using a group of similar random numbers generated from biometric trait to obtain the symmetric key for encrypt and decrypt



Solution for secure data transmission



Future plans



Analyze the state of the authentication system, depending on human condition



Explore the possibility of using the pulse distance as random values for cryptographic system



Construction of simulation system of cryptographic data transmission in body area network

Conclusions

- Proposed:
 - Authentication system using heart sounds as biometric traits
 - Cryptographic system using characteristics of circulatory system for generation a common key
- Developed:
 - Method of extracting individual characteristic of heartbeat sound signal
- Created:
 - Classification scheme of individual characteristic for making a decision

Questions?

Ekaterina Andreeva

Department of Information Security Technologies

E-mail: eandreeva89@gmail.com

