NOISEPROOF ENCIPHERING OF TRANSFER OF BIOMEDICAL SIGNALS IN TELEMEDICINE TECHNOLOGIES

[1]Artemenko M.V., [2]Teplova V.V.,

[1]Kursk, Russia, FSEI HE South-West State University, Department of Biomedical Engineering,

[1]Kursk, Russia, Private educational institution of higher education Regional Open Social Institute,

Abstract. *Ways of solution of problems of enciphering at transmission of messages, characterizing biomedical signals, in telemedicine technologies for adoption of diagnostic decisions, based on iterations of codes of Hamming and the random number generator when forming noiseproof messages and keys are offered. It is specified what straight lines and latent characteristics of biosignals are recommended for transfer. The algorithm of coding of the transferred messages differing splitting the message into blocks, independent coding of each block, an artificial noisiness and application of the self-repairing Hamming's codes is given. It is offered to determine a block sequence by individual physical characteristics of the recipient: by voice or fingerprints.*

Keywords: telemedicine, biomedical signals, noiseproof coding of messages.

In diagnostic process of clinical medicine practice of processing of biomedical signals is actively used [1,3]. Essentially diagnostic opportunities due to achievements in the field of the telemedicine [2] allowing to analyze quickly signals experts of a different profile extend. The telecast of biomedical signals assume application of noiseproof coding and encoding of messages. Especially, in case of transfer of convolutions of signals – for example: basic frequencies, the period of the analysis, amplitude with multiple frequencies. Transfer only of information frequencies for the subsequent restoration of a signal with necessary diagnostic (classification) properties is possible.

Together with signal transmission it is offered to transfer information characterizing it [4], for example, such informative parameters as:

- straight lines: frequencies, capacities, the valid and imaginary parts of decomposition of a signal identified by means of Fourier of transformation or harmonious algorithms of the method of the group accounting of arguments (MGDH) – the example is given in [5];
- latent: the first minima and maxima at low frequencies (initial harmonicas), global maxima on all range, minima, adjacent to local maxima (at the interfaced frequencies), functional dependences between the valid and imaginary parts of ranges, frequencies of the first minimum at low frequencies, etc.;
- functional – the biosystems characterizing behavior, capable to make the decision (to react to conditions of internal and external environments) at the moment time according to the accounting of last experience and forecasting of development of the situation.

Ensuring privacy of the transmitted data is carried out due to change of the carrier and forms of transfer in a telemedicine now applied rather seldom as the main type of the data carrier is electronic. This way is rather effective as keys of enciphering change at the time of change of the carrier and are independent of the receiver and the transmitter (unlike the opened and closed keys).

Ensuring necessary level of privacy of the interface is reached: first ensuring privacy of transfer of the pictures code of the interface, secondly – individualization of specialized semantics of the thesaurus of subjects of reception-transmission.

For permission of a number of the specified problems rather simple and effective algorithm of coding of the transferred messages is offered.

1. The text of the message breaks into blocks of various length. The first and last blocks bear information on the nature of breakdown.
2. Each block is coded, the key about coding is attached to other block. Keys of connection are located in parts in each of blocks.
3. The received codes are transformed by means of the self-restoring Hamming's codes.
4. The artificial noisiness of each block and new coding is carried out.
5. Blocks are transferred to the receiver in a certain sequence: or it (is in parallel recommended), or consecutive in parallel, or consecutive ("packs"). The sequence of the block is defined by physical characteristics of the recipient (for example, voice or fingerprints).

Hamming's code is applied to providing a noise stability (or other analog). Thereby the principle for each block "the message-coding Hamming's code-casual noise-coding-Hamming's code (or other)-transfer" is implemented.

Thus, the offered algorithm carries out purposeful anti-jamming coding of the transferred message with high degree of protection of information against the unauthorized access realized on the basis of objective algorithms and subjective factors of the persons which are carrying out and-or controlling information transfer process.

Reference

1. Artemenko M.V., Kalugina N.M. Diagnosticheskij analiz sostojanija bioob#ekta po hronometricheskim parametram registriruemyh signalov // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. 2016. № 4-2 (46). S. 30-35.
2. Kobrinskij B.A. Telemedicina v sisteme prakticheskogo zdravoohranenija.–M.: Direkt-Media, 2016. – 238 s.
3. Rangajjan R. M. Analiz biomedicinskih signalov. Prakticheskij podhod: uchebnoe posobie / R. M. Rangajjan. - M.: Fizmatlit, 2007. - 440 s.

4. Kalugina N. Diagnnostics of the organism on biomedical signals based on reinforcement learning// XII Russian-German Conference on Biomedical Engineering Proceedings of the 12th Russian-German Conference on Biomedical Engineering. 2016. p. 204-207.
5. Artemenko M.V., Podval'nyj E.S., Starcev E.A. Metod kompleksnoj ocenki i vyborka sostava informativnyh priznakov v zadachah ocenki sostojanija biotehnicheskih sistem // Biomedicinskaja radiojelektronika. 2016. № 9. S. 38-44.