Application of Biosignals in the End-to-End Encryption Protocol for Telemedicine Systems

T. I. Buldakova and D. A. Krivosheeva

Abstract The problem of data protection in telemedicine systems is investigated. As an example of such systems, a telemedicine system for remote monitoring of a person's state is considered. The features of the remote monitoring system, an integral part of which is a mobile measuring complex for receiving, recording, and processing human biosignals, are noted. The solutions developed during the monitoring process are based on the received data and the results of their analysis. Therefore, it is necessary to ensure the protection of the transmitted data in remote monitoring systems of the human state. The relevance of research in the field of information security of telemedicine systems is noted and the task of ensuring the integrity, availability, and confidentiality of data is set. To protect personal data, it is proposed to use end-to-end encryption, for which it is necessary to choose a method for distributing cryptographic keys. It is shown that the appropriate processing of the recorded biosignals allows us to obtain the necessary information for constructing keys. The processing is based on the reconstruction of a mathematical model that generates time series that are diagnostically equivalent to the original biosignals. The examples and results of such processing are given.

Keywords Protection of Information · Telemedicine · Biosignals · Reconstruction of System Model

1 Introduction

The modernization of the healthcare system is accompanied by the active introduction of information and communication technologies that ensure the formation of channels of sustainable communication between specialists of different medical and preventive institutions, remote access to medical information systems (MIS), and facilitate and speed up the registration of patients for appointments with doctors [1–4]. An example of the development of virtual healthcare infrastructure is telemedicine systems, which

T. I. Buldakova (✉) · D. A. Krivosheeva
Bauman Moscow State Technical University, 2-ya Baumanskaya, 5, Moscow 105005, Russia
e-mail: buldakova@bmstu.ru

A. G. Kravets et al. (eds.), *Society 5.0: Human-Centered Society Challenges and Solutions*,
Studies in Systems, Decision and Control 416,
https://doi.org/10.1007/978-3-030-95112-2_3

remotely provide patients with highly qualified assistance from doctors of leading medical centers [5–7].

In such telemedicine systems for remote monitoring of human health, cloud computing technologies are increasingly used, when a system of wearable sensors is installed on the patient, which registers physiological information (mainly biosignals) and transmits it wirelessly to the server. Medical personnel can view the collected information in real-time in the medical information system containing the biosignal database and assess the current functional state of the patient.

When creating telemedicine systems, an important task is to ensure information security [8, 9]. Such systems process not only personal data, but also demographic, financial, and medical information. Therefore, it is necessary to ensure the security of the personal data processed by the system and the information that constitutes a medical secret.

This issue is particularly acute in remote monitoring of the human state. The lack of real security capabilities can not only lead to data privacy violations but also potentially allow hackers to harm the patient by altering real physiological data, leading to incorrect diagnosis and treatment. Taking into account the international requirements of the *Health Insurance Portability and Accountability Act* (HI-PAA), the protection of personal medical data is absolutely necessary (http://www.hhs.gov/ocr/hipaa/). Thus, the task of improving information protection methods in systems for remote monitoring of a person's state is very urgent.

2 Features of the Telemedicine System for Remote Monitoring of a Person's State

Currently, telemedicine systems for monitoring the human state are becoming more widespread. First of all, they are used for monitoring the state of elderly people, patients with chronic diseases, and in the process of rehabilitation, as well as for assessing the state of operators of cyber-physical systems [10–13].

The modern telemedicine complex is created on the basis of a powerful computer, which is easily interfaced with a variety of medical equipment, means of short- and long-range wireless communication, video conferencing, and IP broadcasting. An important area of development of remote monitoring of the patient's state is the integration of various biosignal sensors into clothing, various accessories, and mobile phones [14, 15].

Sensors that allow registering human biosignals (electrical activity and heart contractions, pulse signal, electrical activity of the brain, external respiration function, etc.), act as sources of primary information. Therefore, a mobile measuring system is an integral part of the telemedicine system for remote monitoring of the person's state. It performs the recording, registration, and primary processing of biosignals.

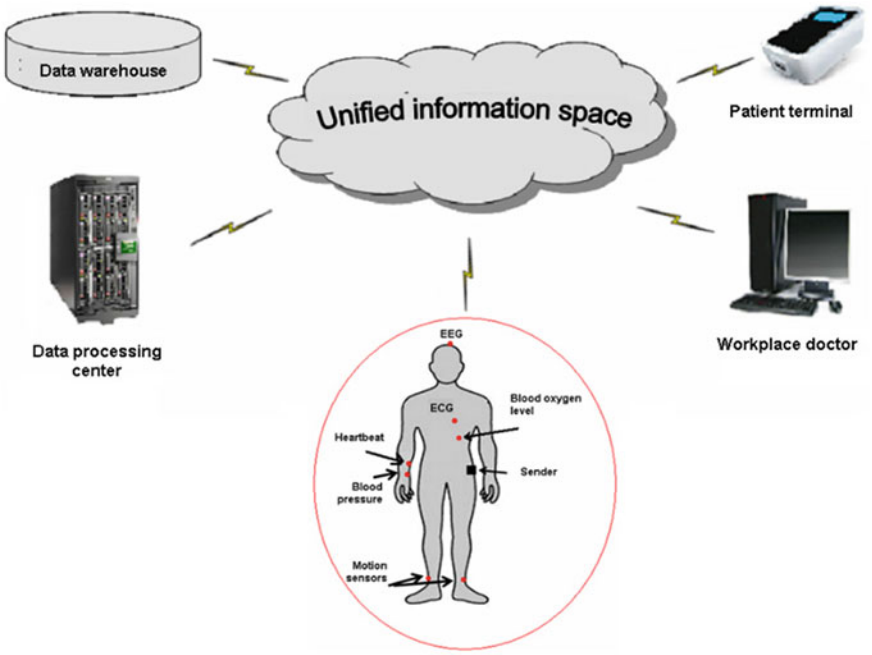

Fig. 1 Organization of remote monitoring of a person's state

The inclusion of such a mobile measuring system in a single information space provides continuous monitoring of a person's state regardless of his location (Fig. 1).

Sensors can send data to the cloud directly or via intermediate base stations. Service personnel and the user can view the collected medical information directly from the cloud using a smartphone or via the Internet in real-time and make decisions in accordance with the current functional state of the person.

However, given the possible access to information (including unauthorized access) of various specialists, methods and technologies are required to protect the personal data of patients.

3 End-to-End Encryption for Sensitive Data Transfers

The created threat model and its analysis showed that there is a problem of ensuring the information security of patient data [16]. At the same time, it is crucial to protect personal medical information when it is transmitted via a communication channel from sensors to a cloud-based medical database.

Unlike traditional systems for monitoring the state of a person, where the server can be reliably protected from external threats, in the technology of "cloud" computing the server is virtual and, in essence, is a rented computing resource

accessible via the Internet. The information vulnerability of such a server is much higher.

The modern approach to securing the transmitted data is End-to-End Encryption (E2EE)—a method of data transfer when only users involved in communication have access to messages.

End-to-end encryption is designed to prevent data from being read or secretly altered by other than the true sender and receiver. Messages are encrypted by the sender, the recipients receive the encrypted data and decrypt it themselves. The third-party has no means of decrypting them. End-to-end encryption prevents attackers from gaining access to the keys needed to decrypt messages.

The E2E protocol works by setting and then distributing cryptographic keys between the sensors and the cloud, which ensures data secrecy and integrity. The main difficulty lies in the possibility of confidential distribution (delivery) of keys to users of the system. In this regard, to protect the transmitted personal information, it is necessary to choose a method for distributing cryptographic keys between the sensor and the cloud to ensure the encryption and integrity of the data.

Let's consider possible approaches to the implementation of the protocol for telemedicine systems.

Traditionally, asymmetric cryptosystems are used to ensure the security of health systems, when two different keys are used: one for encoding, the other for decoding messages (Fig. 2). This is sufficiently reliable to ensure the confidentiality and integrity of the transmitted data [17, 18]. However, for the regular exchange of data in real-time (which is typical for remote patient monitoring systems), this approach is time-consuming and resource-intensive due to the large length of the keys.

The use of paired keys (ie, symmetric cryptosystem) significantly reduces these costs, but there is another drawback—the impossibility of authorization confirmation since the key is known to each party (Fig. 3).

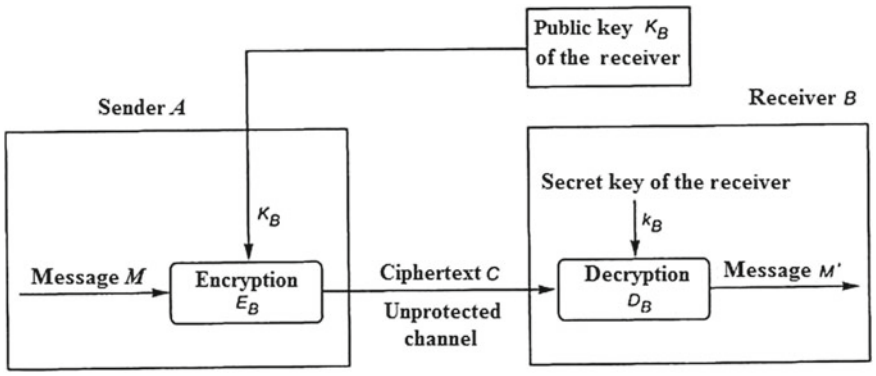

Fig. 2 Data transmission using an asymmetric cryptosystem

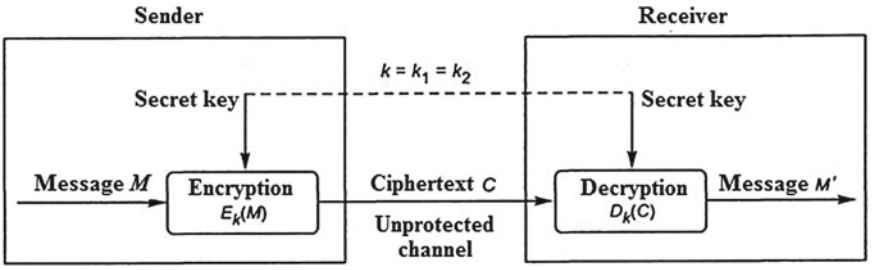

Fig. 3 Data transmission using a symmetric cryptosystem

Thus, to implement end-to-end encryption in telemedicine systems, it is necessary to solve the problem of the covert distribution of cryptographic keys between the participants of the process.

4 Using Biosignals to Hide Information

Currently, there are works that suggest overcoming this difficulty and improving the reliability of symmetric cryptographic keys by using biosignals recorded by sensors. Biosignals reflect the physiological characteristics of the patient and can therefore be used to hide information [19–22]. For example, in [23], some morphological features of biosignals, which are unique to humans and which change little over time, are identified (Fig. 4).

In addition, physiological signals can be artificially generated using a generator model, provided that this model is adequately constructed on the basis of information about the human state [24]. The marked properties of the biosignals make it possible to use them to create keys. The necessary information (morphological features of a particular person's biosignals) is extracted at the first signal registration.

The use of biosignals for end-to-end encryption of data transmitted from the sensor to the object is implemented in the protocol PEES (Physiology-based End-to-End Security). Note that the PEES network protocol using patient biosignals does not require a priori key distribution. To create a secure E2E communication, it is enough to simply install the sensors on a person during the first visit to a medical specialist. In the cloud, inside the storage, the diagnostic equivalent of biosignals is stored in the form of time series created using a model generator, which must be tuned according to the patient's physiological data (Fig. 5).

To implement this approach, it is necessary to choose a method for constructing a model for generating artificial physiological signals. Let's consider two biosignals—ECG and PPG.

In [23], an artificial ECG generator is described by the expression

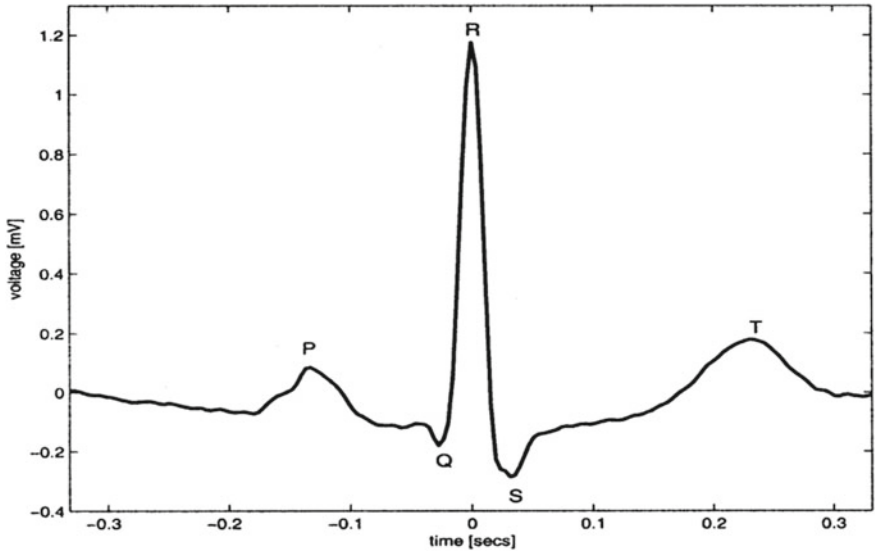

Fig. 4 Morphological *PQRST* parameters of the ECG signal of a healthy person

$$\frac{dECG(t)}{dt} = -\sum_{i \in P,Q,R,S,T} a_i (2\pi hr_{mean} t - \theta_i) e^{\left(\frac{-(2\pi hr_{mean} t - \theta_i)^2}{2b_i^2}\right)},$$

where hr_{mean}—average heart rate of a person. Time-varying parameters include heart rate mean, heart rate standard deviation, and *LF*/*HF* ratio.

To determine morphological parameters, each type of P, Q, R, S, and T waves on the ECG is represented by a Gaussian curve. Each curve has three parameters, and therefore there are 15 morphological parameters (aP, aQ, aR, aS, aT, bP, bQ, bR, bS, bT, θP, θQ, θR, θS, θT).

The photoplethysmogram curve (PPG) is obtained as a result of solving differential equations based on a simple model of the human vascular system—the Windkessel model [25]. PPG is divided into two parts—systole and diastole. Diastole is modeled using the equation:

$$PPG_{dias}(t) = a_1 + a_2 e^{(-a_3 t)} + \frac{1}{a_4 + e^{(-a_5 t - a_6)}} \cdot \cos(a_7 t + a_8). \quad (1)$$

For systole, the analytical expression for the waveform is:

$$PPG_{sys}(t) = \frac{1}{a_9 + e^{(-a_{10} t - a_{11})}}. \quad (2)$$

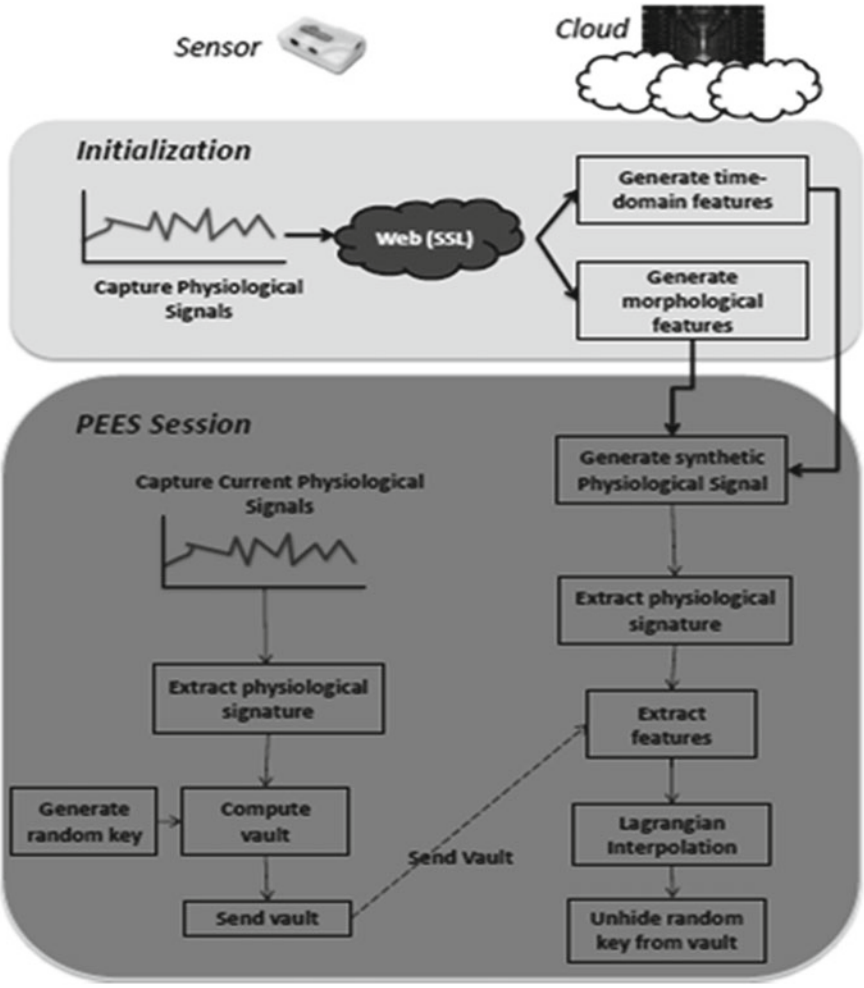

Fig. 5 Provision of information security using the *PEES* protocol [23]

The morphological parameters are the coefficients [a1, a2, …, a11] in Eqs. (1) and (2). Timing parameters include heart rate, heart rate standard deviation, and LF/HF ratio.

In essence, the work [23] used the reconstruction of functional dependencies using time series (biosignal records), where the selection of functional dependencies was carried out based on the shape of the recorded ECG and FPG biosignals. A result is a large number of morphological parameters, which should be considered as a multidimensional characteristic vector (morphological vector). If we take into account that the calculation of these morphological parameters using the least-squares

method is a poorly conditioned task, we come to the conclusion that in practice such a morphological vector does not have the necessary stability.

5 Proposed Solution

To eliminate the indicated drawback of the PEES protocol, it is proposed to use not separate parameters of the time curve, but a mathematical model of a biosignal generator in the form of a system of differential equations, as morphological signs. In this case, the structure of the model and its parameters become morphological features, and the task of determining morphological features is reduced to the task of reconstructing the model of the system. The key generation process is performed in accordance with the PEES protocol and is studied in detail in [23].

The model approach to the analysis of systems using reconstruction has proven itself well in the processing of human biosignals [20]. Let us consider the application of this approach when using a sphygmogram that registers fluctuations in the arterial wall caused by the release of the shock volume of blood into the arterial bed.

In [7, 16], the dynamic properties of the vascular wall are described by the autonomous Van der Pol-Rayleigh equation:

$$\ddot{x} + \left[\varepsilon_1\left(x^2 - r^2\right) + \varepsilon_2\left(\dot{x}^2 - \omega_0^2 \cdot r^2\right)\right] \cdot \dot{x} + ax = P(\omega_0 t), \tag{3}$$

where x—the movement of the artery wall detected by the sensor; $P(\omega_0 t)$—the effect of cardiac activity on the dynamics of the vessel wall; ε_1, ε_2, a, ω_0 and r—model parameters that determine the fluctuations of the blood vessel wall (frequency, amplitude, etc.). In this case, the ECG signal is the input of the model system, and the sphygmogram is the output.

Since the “heart-vessels” system operates in the limit cycle mode, the unknown parameters ω_0 and r of the model (3) can be determined from experimental data, after which the values p_i, a, ε_1 and ε_2 are found using the measured values $x(t)$ and the calculated values $\dot{x}(t)$ and $\ddot{x}(t)$. Here p_i is the coefficients of the expansion of the function P into the Fourier series, where $i = 1, \ldots, N$.

The simulation results are shown in Fig. 6, where the output (pulse) signals of a person and the model system are shown.

The presented results, which demonstrate the similarity of the dynamic behavior of a real object and its model, confirm the good adequacy of the model with respect to the main dynamic properties. In addition, the advantage of the presented model is that the parameter a has a physical meaning: it allows you to evaluate the "stiffness" of the vessels due to the work of the smooth muscles that envelop them.

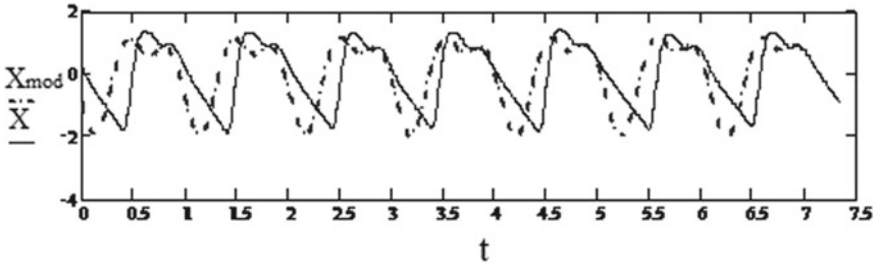

Fig. 6 Simulation results

6 Results

The proposed model (3) makes it possible to take into account various states of a person (Fig. 7) since they correspond to different values of the model parameters a, ε_1, and ε_2. The figure shows that in addition to increasing the frequency, the shape of the biosignals also changes. For example, for a healthy person at rest, the following values are obtained: $\varepsilon_{1\,=}\ -0{,}3$; $\varepsilon_2 = -3{,}37$; $a = 36{,}15$. In a stressful state with an intense load for the same person, the parameters received the following values: $\varepsilon_{1\,=} -1{,}07$; $\varepsilon_2 = -8{,}31$; $a = 95{,}5$.

The parameters of Eq. (3), reflecting such properties of the vessel as compliance and dissipation, are inherent in any vessel and, at the same time, are unique for an individual person.

Thus, it is necessary to embed into the PEES protocol not a large number of morphological features, as was done in [23], but information about the structure of the model equation (for example, Van der Pol-Rayleigh or Van der Pol-Duffing) and also the values of its parameters [16].

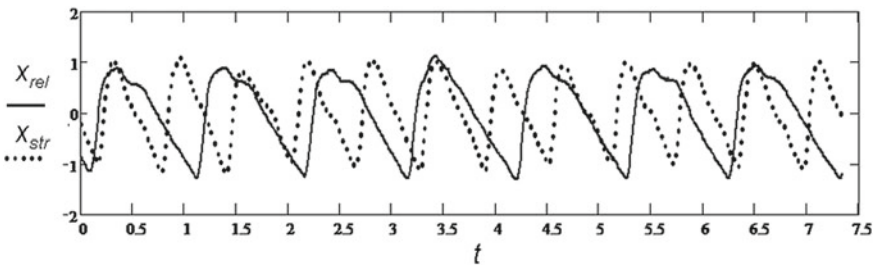

Fig. 7 Pulse signals at rest and under stress load

7 Conclusion

Studies have shown that as a result of the use of biosignals, the efficiency of end-to-end encryption increases and it becomes possible to prove authorship in a symmetric cryptosystem.

An approach is proposed in which a reconstructed mathematical model of a biosignal generator is used to construct cryptographic keys. The data protection method based on this approach is demonstrated by the example of the "heart-vessels" biosystem. It is shown that the model of the pulse mechanism in the form of a reconstructed mathematical model of a biosignal generator can be used in a security system to verify the authenticity of a message by comparing the features of the original and reconstructed signals.

Implementation of this method in monitoring systems will allow not only to improve the adequacy of the patient's state assessment based on multiple non-invasive measurements but also to form morphological signs for the formation of a "physiological" signature of a person. These characteristics include the structure of the model used to assess the human state and its physiologically significant parameters.

References

1. Aleman, J.L., Senor Carrion, I., Toval, A.: Personal health records: new means to safely handle health data? Computer **45**(11), 27–33 (2012)
2. Malasinghe, L.P., Ramzan, N., Dahal, K.: Remote patient monitoring: a comprehensive study. J. Ambient. Intell. Humaniz. Comput. **10**, 57–76 (2019). https://doi.org/10.1007/s12652-017-0598-x
3. Lantsberg, A.V., Troitzch Klaus, G., Buldakova, T.I.: Development of the electronic service system of a municipal clinic (based on the analysis of foreign web resources). Autom. Doc. Math. Linguist. **45**(2), 74–80 (2011)
4. Buldakova, T., Krivosheeva, D., Suyatinov, S.: Hierarchical model of the network interaction representation in the telemedicine system. In: 2019 XXI International Conference Complex Systems: Control and Modeling Problems (CSCMP), Samara, Russia, vol. 2019, pp. 379–383 (2019). https://doi.org/10.1109/CSCMP45713.2019.8976743
5. Bokolo, A.J.: Application of telemedicine and eHealth technology for clinical services in response to COVID-19 pandemic. Health Technol. **11**, 359–366 (2021). https://doi.org/10.1007/s12553-020-00516-4
6. Bashi, N., Karunanithi, M., Fatehi, F., Ding, H., Walters, D.: Remote monitoring of patients with heart failure: an overview of systematic reviews. J. Med. Internet Res. **19**(1), e18 (2017)
7. Suyatinov, S.I.: Criteria and method for assessing the functional state of a human operator in a complex organizational and technical system. In: 2018 Global Smart Industry Conference (GloSIC), Chelyabinsk, Russia, pp. 1–6 (2018). https://doi.org/10.1109/GloSIC.2018.8570088
8. Appari, A., Johnson, M.E.: Information security and privacy in healthcare: current state of research. Int. J. Internet Enterp. Manag. **6**(4), 279–314 (2010)
9. Buldakova, T.I.: Cybersecurity risks analyses at remote monitoring of object's state. In: Kravets, A., Bolshakov, A., Shcherbakov, M. (eds.) Cyber-Physical Systems: Industry 4.0 Challenges. Studies in Systems, Decision and Control, vol. 260. Springer, Cham. (2020). https://doi.org/10.1007/978-3-030-32648-7_15

10. Anishchenko, L., Smirnova, E.: Bi-directional Long Short-Term Memory Networks for Fall Detection using Bioradars. In: 2020 International Conference on Biomedical Innovations and Applications (BIA), Varna, Bulgaria, pp. 1–4 (2020). https://doi.org/10.1109/BIA50171.2020.9244280
11. Ashapkina, M.S., Alpatov, A.V., Sablina, V.A., Kolpakov, A.V.: Metric for exercise recognition for telemedicine systems. In: 2019 8th Mediterranean Conference on Embedded Computing, MECO 2019-Proceedings, art. no. 8760024. (2019). https://doi.org/10.1109/MECO.2019.8760024
12. Prado, M., Roa, L., Reina-Tosina, J.: Virtual center for renal support: technological approach to patient physiological image. IEEE Trans. Biomed. Eng. **49**(12), 1420–1430 (2002)
13. Ushakov, I., Bogomolov, A., Dragan, S., Soldatov, S.: Technology for predictive monitoring of the performance of cyber-physical system operators under noise conditions. In: Kravets, A.G., Bolshakov, A.A., Shcherbakov, M.: (eds.) Society 5.0: Cyberspace for Advanced Human-Centered Society. Studies in Systems, Decision and Control, vol. 333. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-63563-3_21
14. Paradiso, R., Loriga, G., Taccini, N.: A wearable health care system based on knitted integrated sensors. IEEE Trans. Inf Technol. Biomed. **9**(3), 337–344 (2005)
15. Mundt, C.W., Montgomery, K.N., Udoh, U.E., Barker, V.N.: A multiparameter wearable physiologic monitoring system for space and terrestrial applications. IEEE Trans. Inf. Technol. Biomed. **9**(3), 382–391 (2005)
16. Buldakova, T., Krivosheeva, D.: Data protection during remote monitoring of person's state. In: Dolinina O., et al. (eds.) Recent Research in Control Engineering and Decision Making, ICIT-2019. Studies in Systems, Decision and Control, vol. 199, pp 3–14. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-12072-6_1
17. Malhotra, K., Gardner, S., Patz, R.: Implementation of elliptic-curve cryptography on mobile healthcare devices. Netw. Sens. Control 239–244 (2017)
18. Liu, A., Tinyecc, N.P.: A configurable library for elliptic curve cryptography in wireless sensor networks. Inf. Process. Sens. Netw. 245–256 (2008)
19. Venkatasubramanian, K.K., Banerjee, A., Gupta, S.K.S.: PSKA: Usable and secure key agreement scheme for body area networks. IEEE Trans. Inf. Technol. Biomed. **14**(1), 60–68 (2010)
20. Buldakova, T.I., Suyatinov, S.I.: Reconstruction method for data protection in telemedicine systems. In: Progress in Biomedical Optics and Imaging−Proceedings of SPIE, vol. 9448, paper 94481U (2014). https://doi.org/10.1117/12.2180644
21. Safiullina, L.K., Maturov, R.R.: Image processing for biometric scanning of the palm vein pattern. In: Kravets A.G., Bolshakov A.A., Shcherbakov M. (eds.) Society 5.0: Cyberspace for Advanced Human-Centered Society. Studies in Systems, Decision and Control, vol. 333, Springer, Cham (2021). https://doi.org/10.1007/978-3-030-63563-3_3
22. Cherukuri, S., Venkatasubramanian, K., Gupta, S.K.S.: BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In: Proceedings of Workshop on Wireless Security and Privacy, pp. 432–439 (2003)
23. Banerjee, A., Gupta, S.K.S., Venkatasubramanian, K.K.: PEES: Physiology-based End-to-End Security for mHealth. In: Proceedings of the 4th Conference on Wireless Health. Article No. 2. (2013)
24. McSharry P.E., Clifford G.D., Tarassenko L., Smith L.A. A dynamical model for generating synthetic electrocardiogram signals. IEEE Trans. Biomed. Eng. **50**(3), 289–294 (2003)
25. Nabar, S., Banerjee, A., Gupta, S.K.S., Poovendran, R.: GeM-REM: generative model-driven resource efficient ECG monitoring in body sensor networks. In: International Conference on Body Sensor Networks (BSN), pp. 1–6 (2011)