Using Preventive Measures for the Purpose of Assuring Information Security of Wireless Communication Channels

Ilya Lebedev, Viktoria Korzhuk, Irina Krivtsova,
Kseniya Salakhutdinova
ITMO University
Saint-Petersburg, Russia
{lebedev, vika, ikr}@cit.ifmo.ru, kainagr@mail.ru

Mikhail Sukhoparov, Daniil Tikhonov
SPbF OAO «NPK «TRISTAN»
Saint-Petersburg, Russia
{sukhoparovm, tikhonovdanil}@gmail.com

Abstract—**The task we consider is counteraction to the information security incidents. The special feature of the described solution is an integrated application of the methods ensuring implementation of the preventive measures aimed at increasing the complexity of information security threat implementation on a compact device. It provides tasks required for support of wireless communication channels in an environment exposed to an information influence. A prototype of the compact device based on form-factor PC-104+ relevant to the set objectives is offered and tested, its operation principles are described. There is an assessment of response to information attacks, and the states of the devices are modeled in various modes and during introduction of additional protection elements.**

I. Introduction

Common use of information and telecommunication systems (ITCS) determines the need in assuring confidentiality, integrity and accessibility of transmitted data. Application of various technologies of computer, global, industrial wireless networks, existence of potential possibilities of effecting passive and active attacks from outside do not warrant the full safety of transmitted data.

More and more important direction of development of information security becomes the improvement of the theory and practice of constructing decentralized intelligent information security systems.

The decentralized nature of information systems and the potential for communications make functional environment most vulnerable for such threats like an unauthorized interception of communications, violation of the integrity of transmitted data over the network, unauthorized access, denial of service (DDoS-attacks), intercepting requests and their subsequent modification and reproduction, etc.

Therefore, more attention is paid to systems that can respond to various incidents of information security, for example, to carry out the change of data transmission channels, encryption keys when the event occurs the appearance of "repetitive" messages, bad frames.

Typical solutions on introduction of cryptographic tools do not always let achieve the set level of protection and, in most cases, require additional arsenal of methods to decrease the likelihood of overcoming the protection.

Therefore there is a need in searching for new software and hardware solutions to prevent information security incidents ensuring implementation of the preventive measures for the information protection [1], [2].

Opportunity for realization is connected with the vulnerabilities at algorithmic and program level, at resources level, which assessment can be carried out by the classical approaches and the information security (IS) methods applied to information systems. At the same time there is a question of the protected condition of the information system having a management structure in case the part from her elements has undergone attack.

It is possible determine the following prerequisites defining a possibility of attacks at management structure level:

- absence, insufficiency, relativity of information on current state, location of each device;
- relatively weak intensity of exchange of information with the coordinating center;
- initially incorporated autonomy of actions of separate elements;
- a possibility of actions of separate elements out of a controlled zone;
- the imperfection of mechanisms of identification and authentication of elements leading to considerable delays at detection of intrusions;
- limited opportunities means of detecting abnormal behavior of elements of information system.

II. Problem Setting

The possibility of realization information security threats in relation to information systems is considered at the algorithmic, program, resource level. Features of system allow to distinguish a number of categories of the potential attacks aimed at violating the integrity, confidentiality and availability of information for which is insufficiently elaborated protection mechanisms:

- information gathering;
- unauthorized access attempts;
- denial of service;
- suspicious activity.

Obtaining the analytical dependences allowing to identify abnormal activity or manifestation of the information events requiring attention, not always perhaps. Therefore there is a need of modeling of system for the purpose of the analysis, state monitoring, and identification of signs of abnormal behavior of separate elements.

The studied system consists of a set of the same type elements. To each element corresponds a tuple, defining his technical characteristics depending on environment, information and technical influences and other factors, allowing to predict his state in system. A tuple is defined by values of internal and external indicators. Internal - are available only to the itself element for making decision on further behavior, external are used by nearest surrounding elements. Change of a condition of one element influences a condition of all system in general.

Existing wireless communication channels, peculiarities of application and operation in an aggressive information environment define a number of solution concepts to be introduced in the protection systems and means, among which the following ones can be distinguished [1]:

- making sure the communication channels are hidden;
- ensuring confidentiality and integrity of the sent and received information;
- enhancement of stability and survivability of the system in the aggressive information environment.

By consideration of a number of projects involving the use of wireless networks, it is necessary to analyze their technical characteristics for the purpose of identification of the weakest places, evaluating opportunities for interaction devices.

For example, researches of a number of wireless network topologies show the need of the analysis of the organization of reception, processing and information transfer. In practice are often formed "bottlenecks" where the considerable volume of the transmitted data "flown down" to one knot and forms a connection between two elements, adjacent elements can render impact on its availability by communicating information among themselves. In that case it is necessary not only to protect this place using standard approaches on the basis of cryptoprotection, but analyze a condition of information security by implementing preventive measures complicating implementation of a number of attacks.

The increasing requirements for computational characteristics of devices, weight, dimensions and power consumption determine solutions such as single board devices (for example ones based on the PC-104+ form-factor) as the priority.

Fig.1 shows a diagram of information protection unit that ensures execution of the above-listed tasks. The possibility of the referred compact device prototype is the possibility of its standard use not only like a regular coder.

Availability of the event analysis system lets respond to individual information security incidents and, controlling external systems, impede an intruder exerting a destructive effect on the communication channels. Spurious information obtrusion system, in case the throughput capacity of the channel permits this, performs periodic sending of false messages having characteristics of regular packets impeding their analysis for decoding.

The messaging channel selection system allows using several channels differing in their frequency ranges for message exchange leaving a part of the channels in backup for suppression of the known ones or carrying out a Dos-attack.

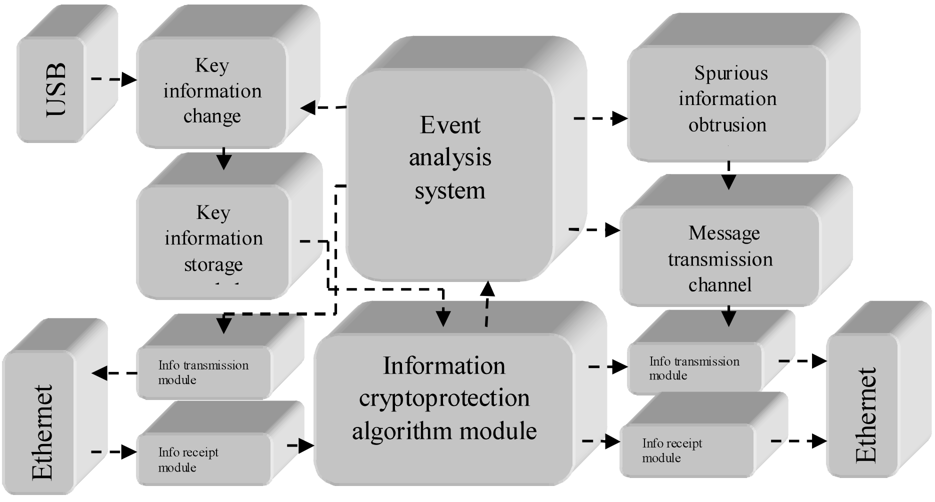

Fig.1. Diagram of information protection unit ensuring solution of security tasks

Thus, the prototype of the device performs:

- control of the information exchange hiding processes by giving commands for using the main and backup frequency ranges, and transmission of false messages mimicking an exchange between the devices;
- control of auxiliary message transmission processes during exchange (splitting the packet into several component parts, sending them via various channels);
- information encryption by standard algorithms;
- introduction of "false" messages to counter the attempts on ripping the code;
- implementation of encryption key change algorithms upon achievement of the pre-defined volume of transmitted information and/or any suspicion on an information security incident;

Introduction and implementation of the above-listed solutions lets respond to a number of "standard" and specific attacks [3,4] targeted to wireless communication channels.

One of the problematic issues in the organization of information security monitoring process is selection of the studied characteristics that are correlated with the probability model of interaction, functioning of remote devices exposed to control of system [13].

To detect abnormal behavior it is necessary to use the characteristics reflecting state of system that can be used in the statistical analysis [15]. For example, it can be:

- response time to a broadcast packet;
- response time to address a package;
- session duration time;
- the number of outgoing packets;
- frequency characteristics of initiation of an exchange of information.

III. Information attack response assessment

A probability theory based approach is selected for assessment of Information Security System structure's response to attack models. The probability density function of a successful carrying out of an attack depends on the probabilities of performance of the following actions by the intruder:

$$P(t) = \prod_{i}^{n} p_i(t) \qquad (1)$$

where the probability density functions $p_i(t)$ i=1,..,n define the intruder's possibilities to intercept, decipher, open the exchange channels and analyze exchange protocols.

Therefore, as shown in the example of possibilities of the prospective devices [1], a number of dependence assumptions can be distinguished for an attack model:

- $p_0(t)$ - probability density of detection and taking advantage of all the channels for attacking.
- $p_1(t)$ - probability density of detection of the right packet in the intercepted traffic.
- $p_2(t)$ - probability density of deciphering the detected right packet.
- $p_3(t)$ - probability density of non-occurrence of the key change even during the system operation.

In order to model an attack, let us assume that the possibilities of opening all channels and key change events undergo the exponential distribution:

$$p_0(t) = 1 - e^{-at} \qquad (2)$$

$$p_3(t) = e^{-\lambda t}$$

where λ - intensity of identified information security incidents of the information security system, a – the parameter determined on the intruder's end by fulfilling attempts to find and take advantage of the exchange channels.

Thus, the probability of an attack undertaking is defined by the expression:

$$P(t) = (1 - e^{-at})p_1(t)p_2(t)e^{-\lambda t} \qquad (3)$$

Fig.2 shows an attack probability curve for various parameters λ and a at $p_1(t)$ →1 and $p_2(t)$ →1, where the encryption key change event occurs over time during a message exchange in the channel.

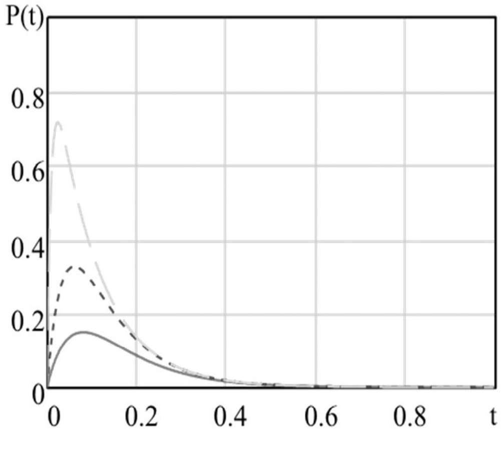

Fig.2. Attack probability curve for various parameters of λ and a

Attempts to use channels by the intruder (spiking of the curves in the beginning of the analyzed period) cause information security incidents identified by the event analysis system, for example, false confirmation backups, duplicating or outstanding packets. As a result of reaching the threshold value (depending on the quality indicators of the information security incident detection) or as soon as the set time comes, the encryption key change events occur.

IV. Device performance assessment

Introduction of additional elements aimed at ensuring response to various destructive effects requires assessment of the device behavior in various modes. Determining the states allows using the Markovian chain device [5], [6], [7]. In order to assess performance of the device in conditions of aggressive information environment, a number of states can be distinguished:

- S_0 – message receipt state.
- S_1 – message processing state.
- S_2 – formation of false reply acknowledgement.
- S_3 – formation of reply acknowledgement.
- S_4 – sending the reply to a channel.

Fig.3 shows a graph of the formation process of false and true messages sent to the channel.

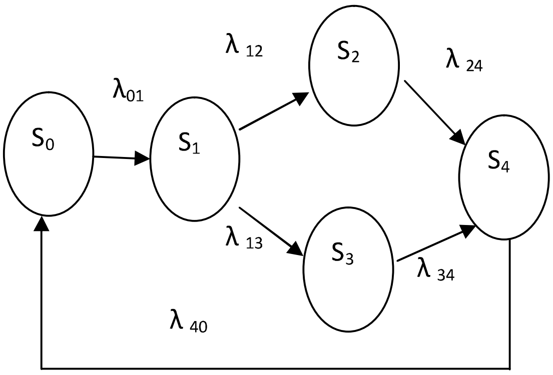

Fig.3. Graph of the formation process of false and true messages sent to the channel

Events leading to other device states may arise not only through the exchange of information between two devices [12].

The intensity of the event, carrying out change of device states can be represented by a system of Kolmogorov equations.

Formula 4 describes states of the devices with the Kolmogorov equation system:

$$\begin{cases} \dfrac{dp_0(t)}{dt} = \lambda_{40}(t)p_4(t) - \lambda_{10}(t)p_0(t) \\ \dfrac{dp_1(t)}{dt} = \lambda_{01}(t)p_0(t) - (\lambda_{12}(t) + \lambda_{13}(t))p_0(t) \\ \dfrac{dp_2(t)}{dt} = \lambda_{12}(t)p_1(t) - \lambda_{24}(t)p_2(t) \\ \dfrac{dp_3(t)}{dt} = \lambda_{13}(t)p_1(t) - \lambda_{34}(t)p_3(t) \\ \dfrac{dp_4(t)}{dt} = \lambda_{24}(t)p_2(t) + \lambda_{34}(t)p_2(t) - \lambda_{40}(t)p_4(t) \end{cases} \qquad (4)$$

Provided that

$$P(t) = \prod_{i}^{n} p_i(t)$$

As appearance of information packets that are unidentified or not corresponding to the current information exchange protocol increases in the channel, the devices come over to state S_2. The probability of being $p_2(t)$ is determined by the expression:

$$p_2(t) = \frac{1}{1+\lambda_{24}(t)(\frac{1}{\lambda_{01}(t)} + \frac{1}{\lambda_{12}(t)} + \frac{1}{\lambda_{40}(t)} + \frac{\lambda_{13}(t)}{\lambda_{12}(t)}(\frac{1}{\lambda_{01}(t)} + \frac{1}{\lambda_{34}(t)} + \frac{1}{\lambda_{40}(t)}))}$$

Fig.4 provides the dependence of the probability of the device being in state S_2 on the intensity of λ_{24} (t) with the rest of the intensity values equal to 1, which enables to evaluate the computational resource required for ensuring intensity of transitions allowing operation of the device and systems ensuring preventive protective measures.

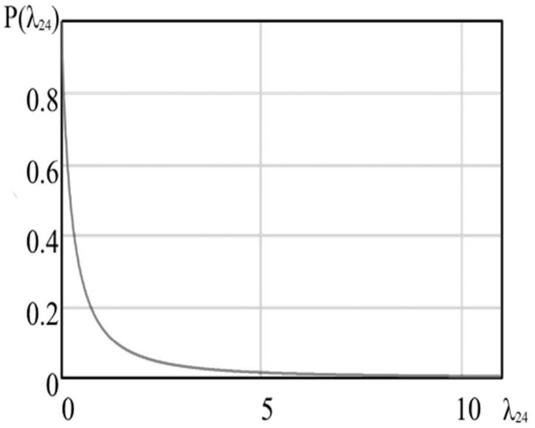

Fig.4. Relationship of the probability of the device being in state S2 on the intensity λ_{24} (t) and the rest of the intensity values equal to 1

V. Static assessment of system of protection

Consider the high-loaded system which is carrying out exchange of information in real time and where packages of data are transferred by a continuous stream.

We will assume that the idle time of the channel is insignificant few *tp*→0. Change of keys is carried out by the entrusted center in advance predetermined function.

Let λ – intensity of change of keys. The probability of implementation of *k* nonsynchronous (attracting emergence of the packages ciphered by a "old" key) changes of keys during time of a broadcast *t* is defined by expression:

$$P(t) = \frac{(\lambda t)^k}{k!} e^{-\lambda t} \qquad (5)$$

Capacity of channel *B* we will determine by expression [9]:

$$B = \frac{L}{ts} \qquad (6)$$

where the *L* quantity of the transferred bits during *ts*.

For an assessment of costs of synchronization of a key we will consider the first case when the transfer is carried out without reinquiry by packages of *w* bits, for example, the video information transmitted over UDP. Consequently, time interval for which it is possible to transfer *n* of packages:

$$B = \frac{nw}{t}$$

$$t = \frac{nw}{B} \qquad (7)$$

At an assumption that the idle time of the channel aspires to 0, the probability of implementation of not less *l* of changes of keys during a broadcast *n* of packages, is defined by expression (6):

$$P = 1 - \sum_{k=0}^{l} \frac{e^{-\lambda \frac{nw}{B}}}{k!} (\lambda \frac{nw}{B})^k \qquad (8)$$

The analysis of expression (8) shows growth of probability of receiving the information packet ciphered by a "old" key when functioning in system of a "new" key. In case of growth of length of an information message.

It allows to estimate the overhead costs connected with the length of the encryption block in symmetric systems of encryption.

Results of modeling of values of probability of emergence of the packages ciphered by an old key from package length in the protocol without confirmation are given in Fig.5.

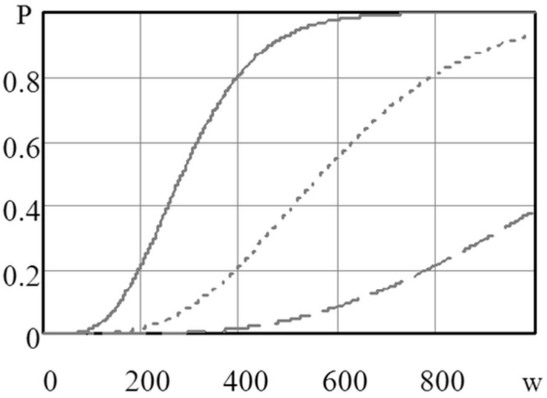

Fig.5. Results of modeling of values of probability of emergence of the packages ciphered by an old key from package length in the protocol without confirmation

In case of existence in protocols of confirmation it is possible consider system when the receipt comes for each information package. Expression (7) will take a form:

$$B = \frac{nw + ncw}{t}$$

where *c* – coefficient of the ratio of the length of the receipts to length of the transmitted messages.

Time which will be required on a broadcast *n* of information packages, will be defined by expression:

$$t = \frac{nw(1+c)}{B}$$

Expression (8) will take a form:

$$P = 1 - \sum_{k=0}^{l} \frac{e^{-\lambda \frac{nw(1+c)}{B}}}{k!} (\lambda \frac{nw(1+c)}{B})^k$$

Values of probability of emergence of the packages ciphered by an old key from package length in the protocol with confirmation for various speeds are given in Fig.6.

With growth of the size of information package when changing a key of enciphering increases emergence of this event at transfer of a package.

In this way, the probability of receiving the information packet encrypted by a "old" key when functioning in system of a "new" key increases.

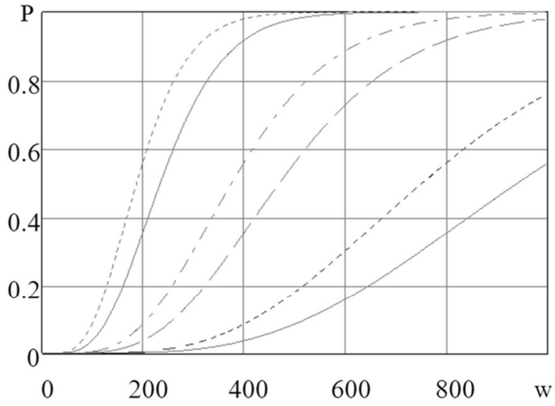

Fig.6. Values of probability of emergence of the packages ciphered by an old key from package length in the protocol with confirmation for various speeds

VI. Experiment

The objective of the experiment was to find the dependence of qualitative indicators of the packets sent by the system when the encryption key is changed. For this purpose, a whole number of actions was performed on the MK-309 based software and hardware information protection unit, which involved synchronous change of keys on two devices.

The purpose of experiment consisted in obtaining dependence of quantitative indices of the packages sent by system for various operating modes.

- setting of the algorithm change the encryption key;
- formation of a recurrent sequence of data for the information fields of packets;
- the choice of length of a package of data taking into account features of symmetric algorithm of enciphering;

- sending packages through a transparent encoder;
- reception and processing packets in the Cryptographic Information Protection Facility (CIPF);
- analysis and comparison of results.

Fig.7 shows a relative frequency of packets received as a result of the experiment encrypted with an old key as soon as the key change event occurs in the system from the length of the packets at various exchange speeds.

VII. Conclusion

One of ways of protection against network threats on perimeter of object of informatization – using a network cryptographic protection of VPN technologies which are based on the tunnel mode of enciphering and which protect object from the active or passive threats directed from an open network.

Unlike linear encoders network encryption technology implemented crypto routers, does not allow to eliminate the threats of analysis and evaluation of the parameters of network traffic.

For example, when using VPN as a part of a telecommunication network of special purpose technical intelligence can be installed the composition of the software on a communication node and disclosed it function and location in the control system.

Measures of counteraction must take into account the research of results methods of network traffic analysis in terms of ensuring the required reliability of identification of the object of intelligence and model of opportunities of investigation.

By consideration of a number of the projects assuming use of information systems, it is necessary to analyze their technical characteristics for the purpose of identification of the weakest places, an assessment of opportunities for interaction of devices.

Thus, the article provides a solution allowing responding to information security incidents.

The novelty is in the integrated application of a number of methods in the information protection system to ensure implementation of preventive measures aimed at the complexity increase of the information security threat implementation on a compact device. The solution of the task is in accomplishing a number of steps associated with collection, analysis and accumulation of statistical data.

The provided solution has a number of advantages driven by the simplicity of implementation not requiring high computational costs, ensuring stability to opening of information transmission channels in a set period of time.

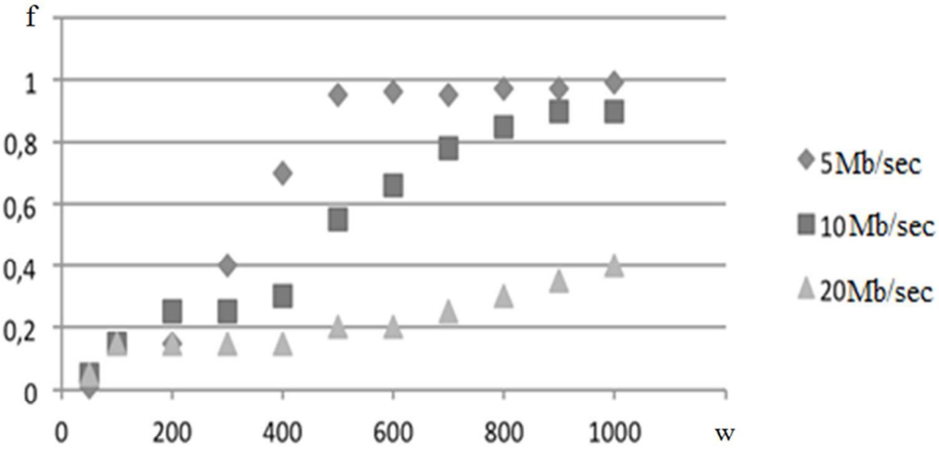

Fig.7. Relative frequency of received packets encrypted with the old key from the length of the packet at various exchange speeds

References

[1] A.M. Wyglinski, X. Huang, T. Padir, L. Lai, T.R. Eisenbarth, and K. Venkatasubramanian, “Security of autonomous systems employing embedded computing and sensors”, *IEEE Micro* 33 (1) 2013, art. No. 6504448, pp. 80-86.

[2] A.V. Gvozdev, I.A. Zikratov, I.S. Levedev, S.V. Papshyn, and I.N. Solovyov, “Predictive assessment of software architecture protection”, *Scientific and technical journal of information technologies, mechanics and optics.* 2012, No. 4 (80), pp. 126-130.

[3] G.N. Maltsev and V.V. Dzhumkov, “Generalized model of discrete information transmission channel with error grouping”, *Information and control systems*, No.1, 2013, pp. 27-33.

[4] Zikratov, I. Lebedev, and A. Gurtov, “Trust and reputation mechanisms for multi-agent robotic systems”, *Lecture Notes in Computer Science*, Volume 8638, 2014, pp. 106-120. (Proc. of the Internet of Things, Smart Spaces, and Next Generation Networks and Systems).

[5] M. Prabhakar, J. N. Singh, and G. Mahadevan, “Nash equilibrium and Marcov chains to enhance game theoretic approach for vanet security”, *International Conference on Advances in Computing, ICAdC* 2012; Bangalore, Karnataka; India; 4 July 2012 through 6 July 2012, Volume 174 AISC, 2013, pp. 191-199.

[6] N. Bazhaev, I. Lebedev, V. Korzhuk, and I. Zikratov, “Monitoring of the information security of wireless remote devices”, *9th International Conference on Application of Information and Communication Technologies (AICT)*, 2015, pp. 233-236.

[7] V. Korzhuk and I. Lebedev, “The monitoring of information security of remote devices of wireless networks”, *15th International Conference, NEW2AN 2015, and 8th Conference, ruSMART 2015*, St.

Petersburg, Russia, August 26-28, 2015, Proceedings, pp. 3-10.

[8] Korzun D.G., Nikolaevskiy I., Gurtov A.V., “Service Intelligence Support for Medical Sensor Networks in Personalized Mobile Health Systems”, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015, Vol. 9247, pp. 116-127

[9] Recommendations MSA-T X.805. Security architecture for systems providing communication between end devices.

[10] Nikolaevskiy I., Lukyanenko A., Polishchuk T., Polishchuk V.M., Gurtov A.V., “isBF: Scalable In-Packet Bloom Filter Based Multicast”, *Computer Communications*, 2015, Vol. 70, pp. 79-85

[11] Kulikov E.I., “Applied statistical analysis: a manual for universities”, *second edition, M.: Goryachaya liniya – Telecom*, 2008, 464 pp.

[12] Komov S.A., “Terms and definitions in the field of information security”, *M., AC-Trast*, 2009, 304 pp.

[13] Kumar P., Gurtov A.V., Linatti J., Ylianttila M., Sain M, “Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments”, *IEEE Sensors Journal,* 2015, Vol. PP, No. 99, pp. 1

[14] Al-Naggar Y., Koucheryavy A. “Fuzzy Logic and Voronoi Diagram Using for Cluster Head Selection in Ubiquitous Sensor Networks”, *Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 14th International Conference*, NEW2AN 2014 and 7th Conference, ruSMART 2014 Saint-Petersburg, Russia, August 27–29, 2014, Proceedings. Springer, LNCS 8638, – PP. 319–330.

[15] Chehri A., Hussein T. “Moutah Survivable and Scalable Wireless Solution for E-health and Emergency Applications”, *In EICS4MED 2011. Proceedings of the 1st International Workshop on Engineering Interactive Computing Systems for Medicine and Health Care,* Pisa, Italy. – 2011. – PP. 25–29.

[16] Kucheryaviy E.A., Ometov A.Y., Andreev D.S., “On the role of wireless technologies in the development of the Internet of Things”, *Information technology and telecommunications*, 2014, N 3 (7), 31–40 pp