

Analysis of the State of Information Security on the Basis of Spurious Emission Electronic Components

Ilya Lebedev, Nurzhan Bazhayev, Mikhail Sukhoparov, Vadim Petrov, Andrey Gurtov
ITMO University

Saint-Petersburg, Russian Federation

lebedev@cit.ifmo.ru, nurzhan_nfs@hotmail.com, mikhailsukhoparov@yandex.ru, petrovvu2005@rambler.ru, gurtov@cs.helsinki.fi

Abstract—The article deals with an approach to determining the state of information security based on the analysis of spurious emission of electromagnetic components. Attention is drawn to the possibility of the formation of the data, obtain samples for the analysis of the state of the information security. An experiment in result of which the amplitude-frequency characteristics of the analyzed radiation. Formed data tuples estimated probability values correctly determine the state on the basis of the data obtained.

I. INTRODUCTION

Construction of protection mechanisms offering counter specific attacks gradually transformed into one of the most important tasks at the various stages of the life cycle of the automated systems.

From the decision making to develop the system before the moment of decommissioning there is a need of constant monitoring and forecasting its various characteristics and indicators. The expert methods applied for these purposes.

Most of the approaches to the construction of mechanisms of protection involves the identification, detection, identification parameters unforeseen external events (wrong addresses, cocked flags messages and connection requests, unpredictable traffic growth). However, the data analysis of events at low levels in order to identify information security incidents is a challenge even for experts, require knowledge of networking protocols, specialized algorithms functioning devices specific manufacturers.

Software data protection consume server resources, workstations, low-power networking nodes, thereby increasing the load on them, slowing down, increasing the technical requirements for the system.

The remote devices of the wireless networking, automated process control system, detectors and transceivers for the operation of the infrastructure of information systems smart cities, outside the controlled area, is the need to improve the development of embedded and external information security tools (IST) using additional channels to assess the state of information security.

One of these "independent channels", supplying information about the status of the remote device information security may be accompanying the operation of the electromagnetic radiation of the radio.

II. A GOAL SETTING

Components of the software - hardware complexes, providing functioning of the various instruments and devices, allow for the reception, processing and transmission of various information. With the introduction of complex information security systems can occur a number of issues related to need to change the network architecture and increasing computing power of the individual units.

At the same time, the functioning of most of the components associated with configuration capabilities that define the use of different types of energy-intensive components.

At the initial stage of operation, after deployment, you can appreciate the different characteristics of the intensity of the information, service packs, query response times, frequency of unrecognized and missed messages. Therefore, one of the possible approaches to identify anomalous behavior - the use of the data reflecting the state of the system, which can be used in the statistical analysis [1].

The test characteristics can be obtained as a result of active and passive surveillance interrogation devices.

Thus, it is necessary to determine the abnormal condition relative to the "normal" functioning based on the statistical characteristics of the data set of elements of the controlled system.

The problem of transient electromagnetic pulse emanation standard (TEMPEST) by means of computer technology as a channel of information leakage has long been known. It needs to develop methods of data analysis states software and hardware systems, identification feature space within the constraints (electromagnetic compatibility, performance, climate, etc.) imposed by the peculiarities of operation of the facilities.

At the initial stage it is possible to evaluate the different characteristics of side electromagnetic radiation and interference caused by the processing of information, service packs, solving computer problems.

In this regard, one approach detecting abnormal behavior - using the digitized data from the processing side emanations received in different system states.

In this article is considered the inverse problem. According to statistical information provided as a result of digitizing the signal, generated electromagnetic, quasi-static magnetic and electric fields to determine the state of information security systems.

III. THE PROPOSED APPROACH

To measure a signal you can use the system of varying complexity. Approach selected depends on the information that must be extracted from the signal.

The simplest case involves the consideration of the two states of the system: the safe state, which function only advance the permitting process and a state in which an uncontrolled process was launched.

To assess the state of information security can be considered the observation interval in order to detect changes in a rented signal obtained as a result of the intensity of the use of electronic components: CPU, memory chips, data bus, and various controllers. As a consequence of using a sequence of rectangular pulses of short duration, it is considered that for the PC are recorded radiation in the range up to 1 GHz, with a maximum in the band of 50 MHz-300 MHz.

In contemporary devices the output signal is represented as a discrete one-dimensional or multidimensional arrays.

Therefore, to assess the state of information security is considered an analysis by a finite number of sample values of a random variable, which is kind of known distribution is assumed, defined parameters of this distribution [2].

As statistics consider amplitude characteristics of side electromagnetic radiation and interference arising from the operation of the electronic components of the PC [3].

IV. A DATA FORMATION

Implementation of information security threats linked to increasing the probability of finding the device in a state that makes it possible to identify the attack.

The analysis of statistical characteristics of a particular device provides the data from based on constructing systems of protection against unauthorized access mechanisms.

Many works devoted to the definition of the information security, for the information, mainly using internal diagnostic system. As the achievement of a functioning point is given information about the predefined parameters for the analysis software -Hardware environment. Based on the values of these indicators to draw conclusions about the normal functioning or the occurrence of anomalies.

However, an incorporation of such systems, delivering data and conducting analysis of information security, causes on the one hand the need to spend additional computing resources, and on the other hand - requires efforts to implement and debug operation of a part of a complex software system.

The possibilities of modern pickup devices and analyzing collateral electromagnetic radiations (EMR) allow to solve a number of specific tasks for reproduction of processed information. For research TEMPEST comprising measuring receivers and spectrum analyzers. Analysis of the amplitude, frequency characteristics of signals at relatively long time intervals provides opportunities to identify specific events occurring associated with the processes of receiving, transmitting and processing.

The Fig. 1 shows a typical circuit that can be used to digitize the frequency indicators, time and signal amplitude.

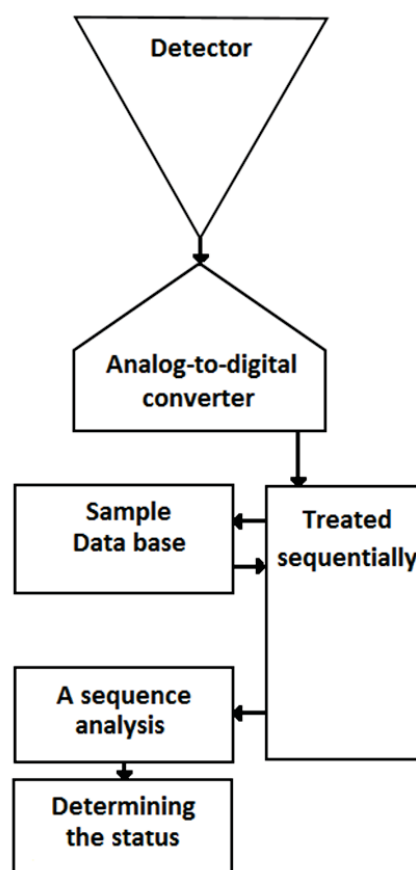


Fig 1. Scheme digitization and analysis of parameters of the frequency and amplitude of signals

The classical approach to information security technical means aimed to suppress a wide range of frequencies of EMR of the test hardware. In contrast, the problem arises EMR, analysis with a view to determining the device status.

The solution of the problems of building protection mechanisms implemented systems using techniques and mathematical device of the probability theory, the information security theory, the prototype devices. The large number of

readily available devices, creates the preconditions for the implementation of simple, does not require painstaking preparation of attacks on the network.

The widespread occurrence outside the area makes it a very attractive target for attempts at various types of attacks.

The potential attacker has sufficient opportunities for the organization of eavesdropping and intercept organization simplest attacks on the network.

To do this, we have to solve a number of issues of information security systems. Under the influence of external and internal factors, the system can be in different states.

Depending on the technical requirements of the system state can be defined as dangerous and the other - as safe.

To obtain information about the states of the information system it is necessary to survey the elements for an extended period of time. In view of the features of the use of information security theory is very difficult to do.

When you create a model resorted to a simplification of the real object of study. When building a model for the analysis of selected most characteristic features, and the rest are not considered.

Modern intelligent sensors and actuators with self-diagnostic system that greatly simplify the solution to this problem.

Thus, it is a promising development, intelligent diagnostic blocks that allow to diagnose the state of devices. Servicing can be done on the basis of using a unique statistical profile of the operation of each device.

When this device is read by the radiation caused by the reference input to be measured and the amplitude and frequency characteristics of the output signal. Analysis and processing is carried out by comparing the output signal from the reference exposure characteristics.

Analysis of the information security status of the device is based on the deviation of the reaction device available statistical profile.

Intelligent diagnostic units can be performed in the stationary and mobile performance. Stationary unit is constantly connected to the device must diagnose at regular intervals and transmit data on the channel.

The response data device and processed information may be transmitted.

To implement a system requires constant analysis of the readings of all the sensors, which imposes restrictions on the processing speed and volume of transmitted and stored data. At the same time there are a number of issues on handling the causes of deviation from the norm of functioning parameters and analyze disturbances.

To overcome the above drawbacks it is necessary to build the mathematical models of the processes.

V. AN EXPERIMENT

HP laptop was taken for analysis of the possibilities of classification of information system security.

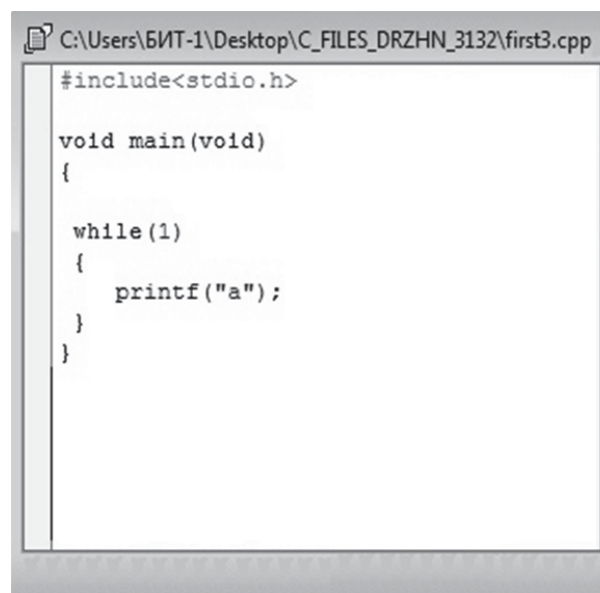
Running OS Windows 7, alternately 2 programs were launched. In the first case, the "eternal cycle" is displayed the symbol "a" in the second case the program algorithm assumes branching register shift left and right, the output of characters on the screen.

The detected programs are in the Fig. 2 and Fig. 3.

The CPU area is the detector connected to the sound card of the second PC, where with the help of the program was carried out the digitization of incoming data. The result was an array.

Each of the features is a vector of values of a variable over time. Depending on the mode change is observed in the statistical portrait of functioning networks and devices.

In view of the low-power devices that provide network infrastructure, evaluation of information security status is easier to carry out, based on the profiles of the normal functioning of the system.



```

C:\Users\BMT-1\Desktop\C_FILES_DRZHN_3132\first3.cpp
#include<stdio.h>

void main(void)
{
    while (1)
    {
        printf("a");
    }
}

```

Fig 2. Simple test program

Formed sample was divided into several parts. The studies were conducted for different ratios of the volume of training and test data.

To analyze the applicability of the methods of search for evidence of the impact of dependency on the probability of correct identification was considered in several modes.

The formation of statistical data based on the analysis of the EMR.

The purpose of the experiment was to obtain quantitative indicators depends on EMR system devices for different modes of operation. To do it, the series of actions were made.

```

C:\Users\БИТ-1\Desktop\C_FILES_DRZHN_3132\first.cpp
#include<stdio.h>

void main(void)
{
int a=0,b;
while (1)
{
b = b << 1;
if (a%2)
printf("a");
else
printf("b");
a++;
b = b >> 1;
}
}
    
```

Fig 3. Test program with branched algorithm

Translation system to the desired operating mode by running corresponding programs.

Analysis and digitizing the data obtained from the received electromagnetic radiation.

Analysis of historical data transfer system and its remote devices in a variety of modes to generate further actions during the experiment and the accumulation of statistics.

In Fig. 4-8 are show amplitude EMR in different computer controller chips.

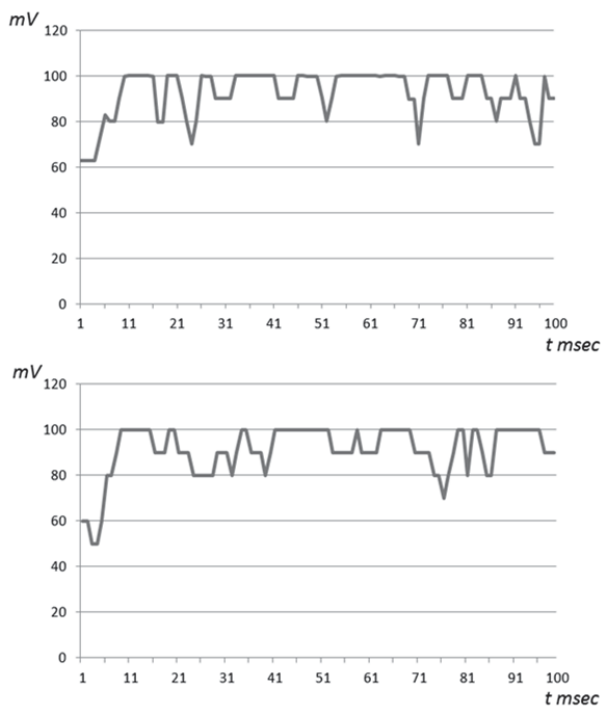


Fig 4. The amplitude of the voltage is removed from the 1 sensor signals 1 and 2 programs

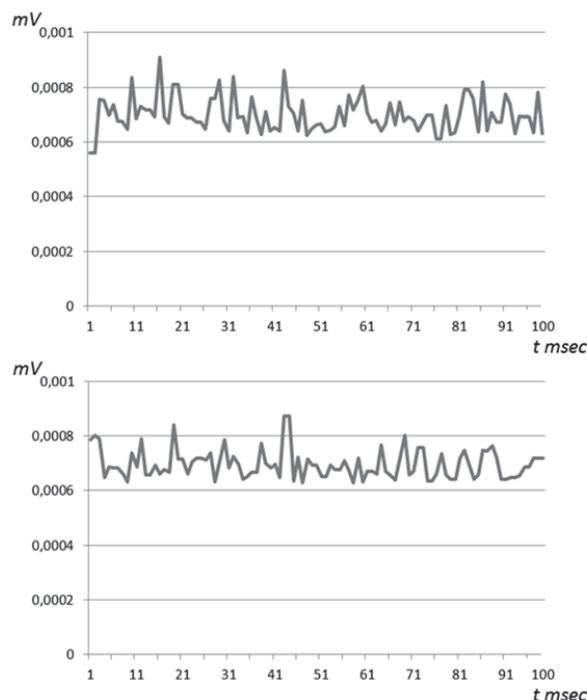


Fig 5. The amplitude of the voltage is removed from the 2 sensor signals 1 and 2 programs

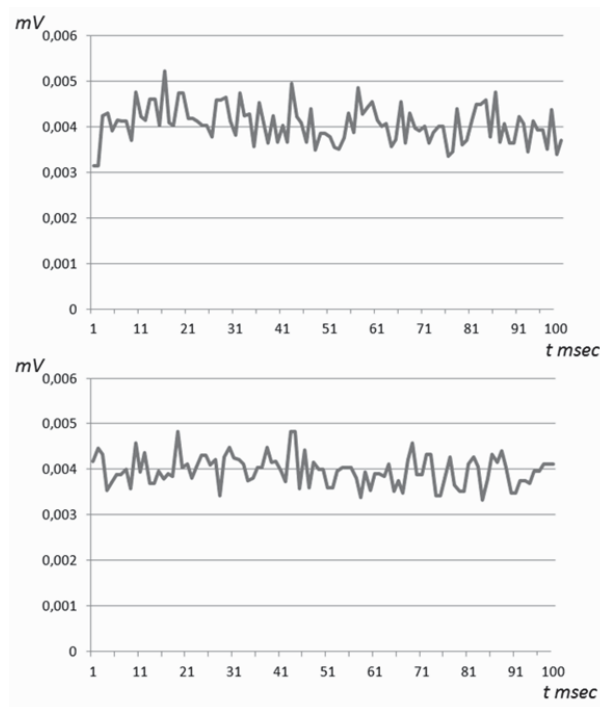


Fig 6. The amplitude of the voltage is removed from the 3 sensor signals 1 and 2 programs

In the first mode of the system training took place on the basis of 250 users messages.

Number of training was tuples 500, 550, 600, 650, 700, 750 from each detector.

The charts shows the values of the frequency and amplitude of the recorded over 1ms.

The graphs of the data for various test programs represented in the figures.

Naive Bayes classifier was implemented in the framework of the experiment. Its advantage is the small amount of training data needed to assess the parameters required for the classification.

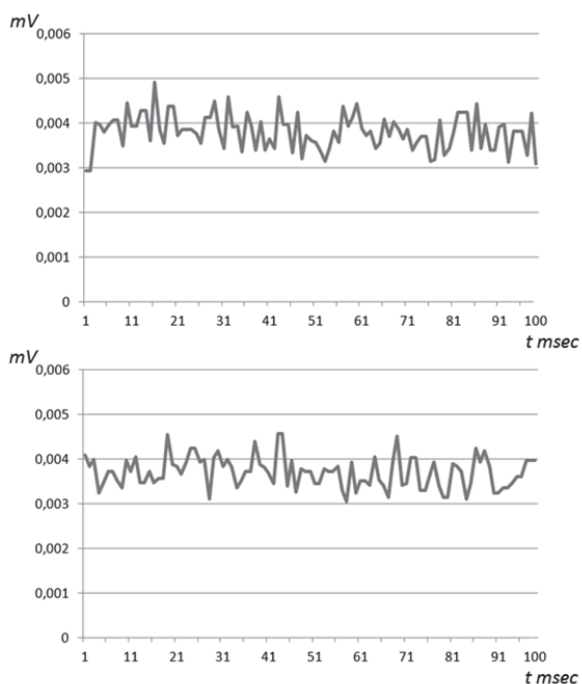


Fig 7. The amplitude of the voltage is removed from the 4 sensor signals 1 and 2 programs

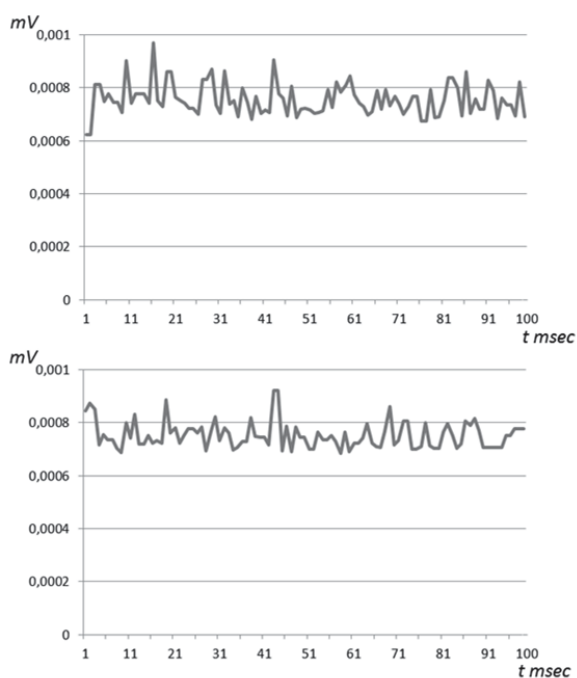


Fig 8. The amplitude of the voltage is removed from the 5 sensor signals 1 and 2 programs

$$C = \arg \max_{h \in H} \frac{p(X/h)p(h)}{p(X)} \quad (1)$$

where h , X - predicted and previous events, and the function p -probabilities of these events and their consequences ($P = m / n$, where the number of the events m - the size, n - number of events)

To form a decision rule used data obtained as a result of digitization:

- The relative frequencies of the classes of the system states;
- The total number of performance features in defined classes for analysis;
- The relative frequency characteristics within each class;
- The number of sample characteristics.

The experiments results are in the Fig. 9.

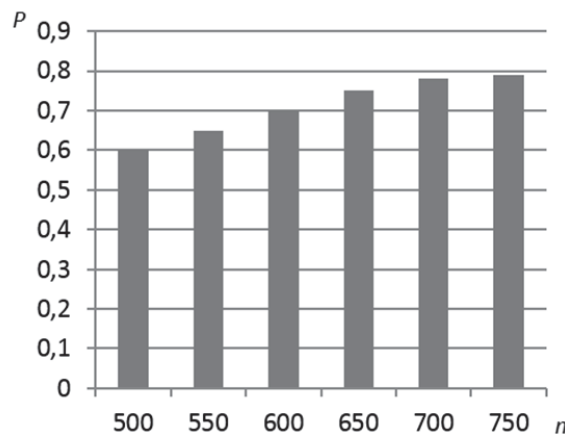


Fig 9. The probability of correct identification of the running program, depending on the volume of training sample

The basis for building mechanisms to protect information is computed on the basis of electro-magnetic radiation of a single circuit element.

The functioning of the information system of protection due to the radiation of a separate analysis of the element in the process of obtaining information from neighboring elements.

To develop algorithms of configuration and automation necessary to measure as many operating parameters and understanding the physical nature of the processes and dynamics that lead to the need to obtain a mathematical model and the application of systems analysis.

VI. CONCLUSION

One of the issues in the organization of information security monitoring process is the selection of the studied characteristics that are correlated with the model of interaction, functioning remote standalone devices subject to control of the system.

The first type of characteristics used to control the system - it is a different identifier, its member units. Information addresses, serial numbers, pre-role devices on the network, the information in the registers. The collection, processing and storage of such information allows you to control the appearance of the "new" devices and detect attempts to introduce foreign elements into the network.

However, there is a possibility of making changes in the algorithm by reprogramming the device an intruder or external pressure on the sensors.

To detect abnormal behavior, use characteristics reflecting the state of the system that can be used in the statistical analysis.

The various modes of operation of the system can be observed anomalies require a more detailed study on the subject of the possibility of unauthorized access.

Determination of quantitative frequency data indicating unrecognized, missed messages, obtain information on the final state of the nodes on the basis of statistical data application layer protocol interaction devices allows for the construction of the side-channel attack system protection mechanisms.

To evaluate the quality characteristics of protection systems against attacks mechanisms necessary to choose a variety of indicators and their groups.

At the same time, the proposed solution does not require large computational cost, such a system can be quickly trained and used as a solution aimed detection of abnormal functioning of the system parameters.

However, even the statistics obtained on the basis of the experiment shows the possibility of determining the probability state of information security for such systems.

The proposed solution can be used to look for anomalies in the functioning of the devices associated with the launch of "complementary" foreign processes.

To improve the accuracy of intrusion detection requires additional analysis of the relationship of the analyzed events.

The proposed approach for monitoring the state of information security devices based on statistical data determined as a result of the digitization of spurious electromagnetic radiation, allows to evaluate the state of information security with the help of probability characteristics.

REFERENCES

- [1] Lee B.H., Kim Y.H., Park K.S., Eom J.B., Kim M.J., Rho B.S., Choi H.Y. Interferometric fiber optic sensors // *Sensors*. 2012. V. 12. N 3. P. 2467–2486. doi: 10.3390/s120302467
- [2] N.A. Bazhayev, I.S. Lebedev, I.E. Krivtsova. Analysis of statistical data from network infrastructure monitoring to detect abnormal behavior of system local segments//*Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, Vol. 17 N1, pp 92–99
- [3] Shamir, E.Tramer. Acoustic cryptanalysis: on nosy people and noisy machines. Eurocrypt 2004 rump session, 2004.
- [4] R. Ortega, A. Bobtsov, A. Pyркиn, S. Aranovskiy, A parameter estimation approach to state observation of nonlinear systems // *Proceedings of the IEEE Conference on Decision and Control*, pp. 6336-6341.
- [5] Wyglinski A.M., Huang X., Padir T., Lai L., Eisenbarth T.R., Venkatasubramanian K. Security of autonomous systems employing embedded computing and sensors // *IEEE Micro* 33 (1) 2013, art. no. 6504448, pp. 80-86.
- [6] Lebedev I.S., Korzhuk V.M. The Monitoring of Information Security of Remote Devices of Wireless Networks // *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2015, Vol. 9247, pp. 3–10.
- [7] Lebedev I., Krivtsova I., Korzhuk V., Bazhayev N., Sukhoparov M., Pecherkin S., Salakhutdinova K. The analysis of abnormal behavior of the system local segment on the basis of statistical data obtained from the network infrastructure monitoring // *Lecture Notes in Computer Science*. 2016. T. 9870. pp. 503-511.
- [8] Bazhayev, N., Lebedev, I., Korzhuk, V., Zikratov, I. Monitoring of the Information Security of Wireless remote devices//*Source of the Document 9th International Conference on Application of Information and Communication Technologies, AICT 2015 - Proceedings* 7338553, Pages 233-236.
- [9] 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.
- [10] Krivtsova, I., Lebedev, I., Sukhoparov, M., Bazhayev, N., Zikratov, I., Ometov, A., Andreev, S., Masek, P., Fujdiak, R., Hosek, J. Implementing a broadcast storm attack on a mission-critical wireless sensor network//*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*Volume 9674, 2016, Pages 297-308.