Advances in Intelligent Systems Research, volume 169
VIth International Workshop 'Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security' (IWCI 2019)

Adaptive Authentication Technologies in Behavioral Analysis Solutions of Robotic Systems

Andrey Iskhakov
V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences
Moscow, Russia
iskhakovandrey@gmail.com

***Abstract*—The paper considers some common aspects of the design of adaptive authentication technology that acts as an executive mechanism in the event of incidents recorded by systems of intelligent control and monitoring. In particular, the author considers in detail the class of User and Entity Behaviour Analytics systems representing an intelligent analytical layer over existing technologies of security and allowing one to identify the deviations in the behaviour of users, and prioritize the recorded incidents. The paper considers in detail the area of application of adaptive authentication technologies in robotic systems. The urgency of the perfection of modern agent authentication methods in mobile robotic groups is defined by the prompt growth of propagation of group robotics in the solution of a wide spectrum of tasks. As a response to the found anomalies in the behaviour of a mobile robotic group agent, it is offered to carry out an additional procedure of authentication, selecting the technique of additional authentication according to the type of the found anomaly and previously constructed profile of a certain subject of access.**

Keywords—authentication, systems of behavioural analysis, adaptive systems, robotic system, DLP, SIEM, UEBA, user's profile, incident, OTP password, information security

I. Introduction

One of the key factors defining the competitiveness of a modern information protection system is its ability to the purposeful adaptation in the conditions of changing of the components and constituents of a protected object, information processing techniques or protection conditions. It is necessary to note that the requirements to flexibility and adaptability of mechanisms are not always due to economic reasons and considerable expenses on the implementation and service of a complex information protection system. Frequently, the given modifications are dictated by the dynamism and uncertainty of the structure of the implementation object. The present paper considers the aspects of the implementation of adaptive authentication technology designed for the integration with the systems of User and Entity Behaviour Analytics (UEBA).

II. The Analysis Of Modern Problems And Their Solutions

A. Traditional methods of authentication

The application of traditional methods of password authentication as a unique system of the authentication of the subject of access has long been considered as an extremely unreliable way of protection against malefactors. The developers try to everywhere introduce the solutions based on multifactor algorithms of authentication [1] to lower the risks of compromising users' accounts. However, this paradigm of protection is based on static rules and leads to strict limitations regardless of the user's identity and the real risks [2]. A vivid example of this is the systems of remote banking. Traditionally, a login attempt into an account of such service is accompanied by OTP-password check. The given password can be generated whether by the bank-client application or received by the subject of access by means of an SMS. Such procedures have become common for the majority of clients, do not cause considerable difficulties and inconveniences in the operation of the application and are extremely seldom exposed to the criticism of end users.

However, the user also needs to enter an OTP to confirm each financial transaction even if it is a common transfer to a regular counteragent or to a close relative. As a rule, the policy of security of a financial organisation provides the requirement to mandatorily execute such procedures with no regard to the device and the place of logging in.

B. Risk-oriented authentication

In this connection, the representatives of large banking systems are actively engaged in the search of solutions in the field of risk-oriented authentication. The given concept means that any factor of authentication has a degree of trust; the choice of the factor of authentication depends on the risk level of a certain operation. Such solutions are certainly extremely important and urgent. On the one hand, they ensure the possibility to protect the client from compromising the account with the help of the analysis of activity of his or her profile whether there are abnormal characteristics; on the other hand, they allow finding the balance between convenience and

reliability, in some cases ensuring the possibility to reduce the number of authentication procedures.

It is necessary to note the following fact: it is enough to use already determined solutions of fraud-monitoring (used in all channels of bank service) for large bank infrastructures to calculate the risk levels of events and the degree of trust of authentication factors whereas for a common user, as a rule, it is necessary to develop a separate analytical subsystem. Thereof, as an intelligent mechanism for user's activity monitoring, it is offered to consider the class of UEBA-solutions. The given class consists of the means of automated analysis of user behaviour on the basis of the data of the access registers for detection of the attacks, for effective prioritising the "operations" of various analysers, and also for helping the information security to effectively respond to threats and investigate incidents.

C. Behavioural Analysis In UEBA-Systems

The behavioural analysis of users and entities as a process of cybersecurity to detect internal threats, attacks or frauds has found high popularity among vendors and experts in the sphere of information security [3]. The reasons of such solutions are obvious enough. The rate of information content circulating in corporate networks and in global cyberspace is rapidly increasing. The competence of malefactors is growing; and constant attempts to steal or modify information in intelligent systems are concealed belter and better. It is becoming extremely complex to distinguish these attempts from regular, legitimate behaviour of users. The combination of the above mentioned factors has led to the development of a new class of solutions – UEBA-modules of information security. In the modern literature, it is possible to define a number of various subdirections of the behavioural analysis of user actions:

- User Behavioural Analytics (UBA);
- Security User Behaviour Analytics (SUBA);
- User and Entity Behaviour Analytics (UEBA).

However, in the given research, the most general common class of the UEBA-systems is considered allowing us to complement the built user profiles with additional data from the system environment (data storage systems, used network infrastructure, lists of applications, etc.).

III. Adaptive Authentication And Its Specifics In the Robotic Systems

A. The place of adaptive authentication in the UEBA architecture

During the preparatory stage, the UEBA-service defines the typical behaviour for each subject and the associated applications, by using algorithms of machine learning. The basic criteria of the typical behaviour are calculated, with the possibility to measure the deviations from the calculated behaviour. Then, constant analysis of actions of each subject is made within the limits of each user's session; the comparison of available models of the user profile to characteristics of undertaken actions is fulfilled with the purpose of revealing abnormal, suspicious or potentially risky behaviour. In the case of detected deviation, the behavioural analysis service starts an intelligent response. In particular, the service can co-operate with the system of incident registration and management to compare the event with similar cases and to offer a target solution with employee's involvement. In addition, such systems keep the retrospective statistics on each user and, based on the obtained data on the user's abnormal activity are capable to somehow evaluate the risk of each of the users. Further, these evaluations are used to rank the events, facilitating the work of the security manager.

The Fig. 1 shows the diagram characterising the place of adaptive authentication procedure execution within the limits of the traditional architecture of UEBA-tools, presented by Gartner [4].

The UEBA-system requires a considerable quantity of data gathered from different sources to carry out an effective analysis. The more information on users is transmitted in the analysis system and the more applications are analysed the higher is the efficiency and speed of detecting the facts of suspicious behaviour. As is shown in Fig. 1, the tasks of gathering and classification of such data are solved by the systems of the class "Security Information and Event Management (SIEM)" that provide an accessible toolkit in its basic configuration for gathering and regular analysis of the big data.

Therefore, the most effective mechanism of implementation of UEBA is their close integration with already existing SIEM-systems [5] which, in turn, use a high number of data sources, ensuring the most possibly complete coverage of the events registered in the IT infrastructure and that of Information Security, and also in the applications of an enterprise. Besides, the manufacturers of UEBA-systems focused on internal threats often use not only system registers as information sources but also the content of correspondence via corporate e-mail and messengers, which allows them to build more detailed and personified models of user behaviour.

Thus, if there exists such an impressive information volume, it is possible to integrate an adaptive system of authentication. The system property of adaptability consists of the ability of a system to adapt to the various conditions. In the given paper, an adaptive technology of authentication is understood as a such set of methods, algorithms and scientific and technical solutions for confirmation of the identified subject authenticity that allows one to inspect, detect and react in real time to the risks of security, optimising procedures of authentication by adjustment of the sets of factors, methods, tools, and criteria of authentication.

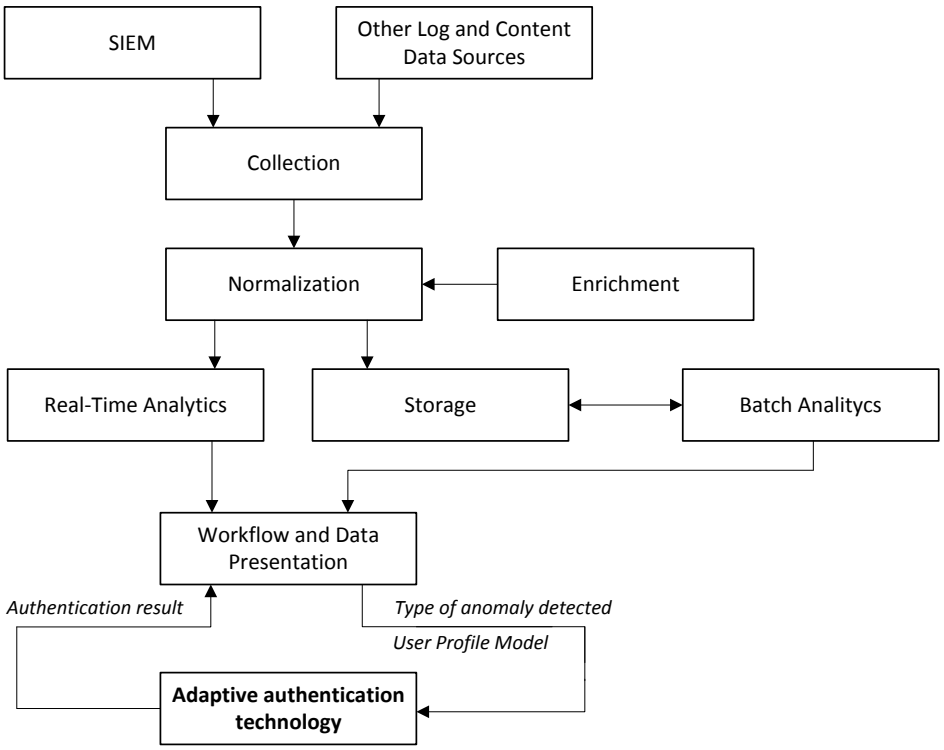

Fig. 1. The application of adaptive authentication technology with UEBA-solutions. The normalised data structures from SIEM-systems and other storages can be used as sources.

As an example let us consider the following scenario of adaptability of authentication procedures. If the security policy of a company allows connecting to the workstation by means of VPN-tunnelling technology with a Remote Desktop service and an employee works from the house from time to time, such logon would not be considered as a risk indicator. At the same time, if the same employee has never gone on business trips and suddenly tries to connect to the system from other country or in an atypical for him or her time interval, the system can use the mechanism of adaptive access control by starting the procedure of two-factor authentication with an OTP password.

Let us consider another example. In addition to external attacks on infrastructure there is a big class of the threats coming from entrusted sources such as legitimate employees of the organisation. These could include leaks of data, internal fraud and exploitation of vulnerabilities in corporate systems to increase the privileges or disable the systems. In such cases, UEBA-systems along with functions of Data Loss Prevention (DLP-tools) can in due time detect the abnormal activity in the user behaviour and react in an appropriate way. For example, when they detect an atypical for a certain subject interaction with corporate systems (for example, export and copying of a considerable quantity of confidential data), they could initiate authentication of a certain operation by means of “a mechanism of authorised representatives” [6]. This mechanism can be realised in the form of a permission request for the atypical operation from a senior employee of the organisation.

B. Aspects of secuity provision in robotic systems

The urgency of the application of modern agent authentication methods in mobile robotic groups is defined by the prompt growth of propagation of group robotics in the solution of a wide spectrum of tasks. However, the application of the mentioned approach in the field area of robotic group agents. Moreover, today there objectively exists the lack of methodological support for the development of the safe environment for data exchange between agents in such groups.

An individual and vital aspect of security provision for intermachine interaction in multi-agent robotic systems is considered in the works by I.I. Komarov, A.P. Zhuk, I.A. Zikratov, L.V. Qiuyun, R.C. Luo, P.K. Wang, etc. At various times these authors undertook attempts to formulate the requirements to perspective mechanisms of information security provision for swarm systems [7-9].

The remote control in such systems is carried out at the expense of a wireless communication system which is one of the most vulnerable elements of a robotic complex subject to various threats. Review, substitution, interception and suppression by interferences of the transmitted and controlling information are among such threats.

A number of investigations [10-12] directed on the increase of efficiency of mobile robotic groups capable to co-operate with each other during the execution of complex missions, including the carrying out of research, reconnaissance, and also tactical battle missions. Thus, in papers [13, 14] it is assumed that the creation of mixed groups including robots

functioning in various environments (in the air, on land, underwater, above water, underwater), will allow to considerably raise the efficiency of the execution of tasks in view.

As a result of the review of the papers [15, 16] devoted to the topic of attack detection on the mobile robots, it is possible to define three main disadvantages of existing approaches:

- The majority of the systems are based on a signature analysis or on a system of rules. In this connection, there are following limitations: the complexity of detection of new attacks which are not related to the detected templates of the malefactor's behaviour and the necessity to maintain an actual status of a base of rules or sets of signatures.
- The systems based on completely distributed methods of detection require additional amount of energy from the nodes and also additional computing power and they increase throughput capacity.
- When using centralized methods, the node fulfilling the main functions on detection of aberrant behaviour is the weakest part of the system. In the case of its disabling, the operation of the network becomes completely disrupted.

IV. Offered Approach

The offered approach to implementation of adaptive authentication is based on the application of the method of aberrant behaviour detection of a malefactor or several malefactors within the limits of mobile robot group on the basis of the probabilistic method [17]. The main advantage of the given method in comparison with the considered solutions consists in that it does not require the formation of the standard probability distribution, unlike other probability methods. The formation of standard distribution is not necessary because the current values of group nodes are taken to detect aberrant behaviour, then the function of the normal distribution is formed and the confidence interval of values (Fig. 2) is calculated.

In the given diagram $R_1 \ldots R_n$ represent agents of robotic system. The source of the information for the analysis is several storages and each of them is characterised by weight W_i:

- T – the session model of node group possessing the greatest weight W1. The iterative upgrade of the given model is meant at regular intervals;
- M –model of analyzed tags previously trained by one of the algorithms of computer-aided instruction for a robotic agent;
- S – previously defined scenario for the given group of robots.

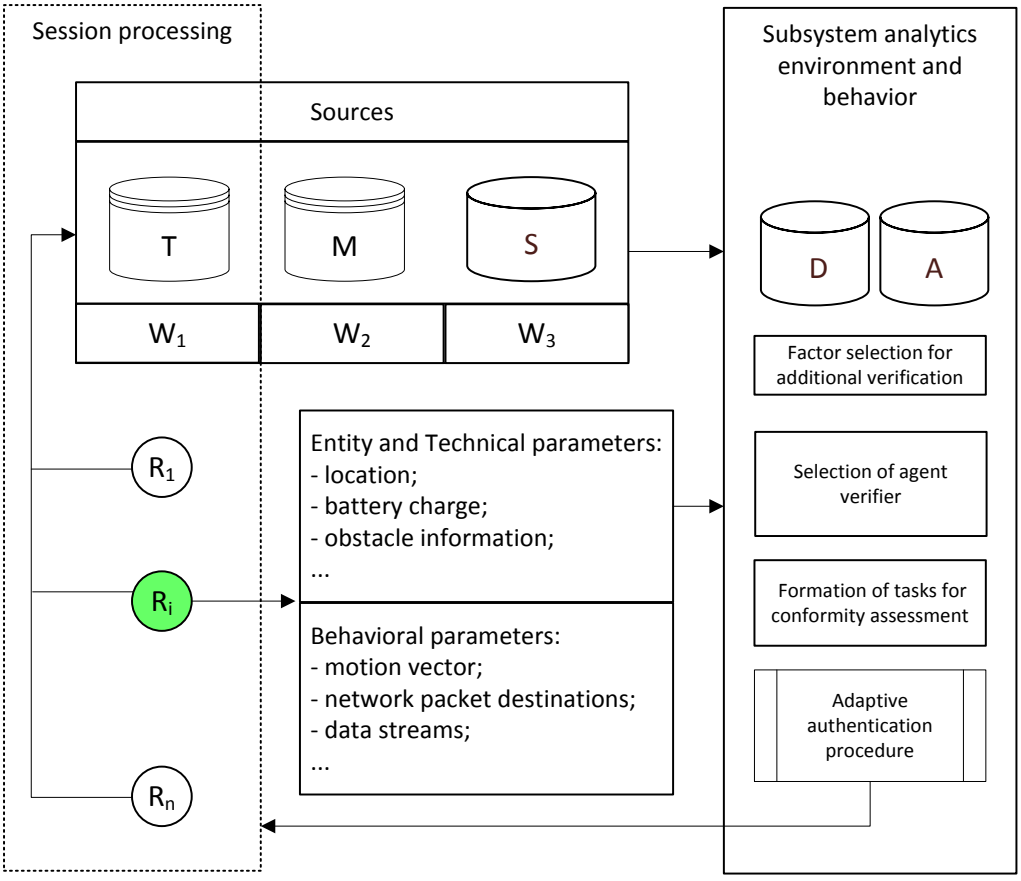

Fig. 2. The diagram of the offered solution. The repetitive process of the behavioural analysis of actions of robotic group agents.

The approach assumes the complex estimation of both the static parameters and the behavioural analysis of the investigated agent R_i. For example, to detect the anomalies in the power consumption of a robotic platform engine, a supervised training algorithm for the certain scenario [18] is offered. Let us assume that the state vector of each robotic agent is described by a set of eight parameters:

$$X_i = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)_i ,$$

where:

- i designates a discrete interval of time;
- the variables x_j are geographical co-ordinates, speed of the mobile platform, the load on the engine, the inclination, the direction and the speed of wind.

To detect the anomalies, the dependence of power consumption of the agent is restored according to its navigation data. The model could be represented by the regression on the basis of a polynomial neural network that could be generally recorded in the form of the ratio to the required degree of nonlinearity:

$$y_i = A_0 + (x_{1,i} , x_{2,i} , \ldots, x_{8,i})A_1 + (x_{1,i}^2, x_{1,i} x_{2,i} , \ldots, x_{2,i}^2, x_{2,i} x_{3,i} , \ldots, x_{8,i}^2)A_2 + \ldots .$$

A_k designates the vector-column of numerical parameters with the dimensionality corresponding to the vector of nonlinearities of the k order. The calculation of these parameter is carried out by the least square method minimizing the mean-square deflection error of the y_i forecast on real power consumption of the given agent $x_{9,i}/x_{1,i}$. Let us note that the equations can have various a state vectors, as different robots can have different sensors (lidars; gyroscopes; accelerometers; sensor controls of the characteristics register of the engine operation, etc.).

Further, the analysis subsystem is based on two main sources:

- D – set of deviations from the profile in the time model of the agent, the long-term model of the group, the general scenario (taking into account the weighting factors);
- A – set of authentication factors weighting factors.

After carrying out the complex analysis in the case when the suspicion appears that the control system of the investigated robot is compromised, the factor of authentication is selected. Further, an entrusted agent is selected and for it, the task to carry out the procedure of adaptive authentication is formed.

V. Conclusion

The industry of development in the field of information security control automation of enterprises needs to solve a number of problems to increase the efficiency of processes of detecting and responding to security incidents and threats. One of such problems is solved by the systems of behavioural analysis. The extension of the functions of such tools by the resources of adaptive authentication is thus important [19]. The necessity of authentication, a set and type of the factors required for authentication of a certain subject should be defined on the basis of the estimation of the risk of a threat during the atypical behaviour of a client in the real-time mode.

An important feature of the offered technology of adaptive authentication in terms of the problem of providing complex information security of an object consists in the fact that the UEBA system constantly controls the user's session (unlike traditional tools with an one step verification of the subject of access during the login).

Acknowledgment

The reported study was partially funded by RFBR according to the research project № 19-08-00331.

References

[1] A.Yu. Iskhakov, R.V. Meshcheryakov, “User authentication schemes in the access control system using QR codes and NFC data transmission”, Information countering the threat of terrorism, vol. 22, 2014, pp. 11-15 [“Skhemy autentifikacii polzovatelya v SKUD s ispolzovaniem QR kodov i peredachi dannyh po tekhnologii NFC”, Informacionnoe protivodejstvie ugrozam terrorizma, vol. 22, 2014, pp. 11-15] (In Russian).

[2] A. Brodsky, “Risk-Based Authentication”, BIS Journal, vol. 2(29), 2018 [“Risk-orientirovannaya autentifikaciya”, BIS Journal, vol. 2(29), 2018] (In Russian).

[3] A.Yu. Iskhakov. A.O. Iskhakova, R.V. Meshcheryakov, R. Bendraou, O. Melekhova, “Application of User Behavior Thermal Maps for Identification of Information Security Incident”, SPIIRAS Proceedings, vol. 6(61), 2018, pp. 147-171.

[4] Gartner. UEBA tool architecture, URL: https://www.gartner.com.

[5] A. Matveev, “Market Analytics of the Behavioral Analysis Systems – User and Entity Behavioral Analytics (UBA/UEBA)”, Anti-Malware, November 2017 [“Obzor rinka sistem povedencheskogo analisa – User and Entity Behavioral Analytics (UBA/UEBA)”, Anti-Malware, November 2017] (In Russian).

[6] A. Yu. Iskhakov, “Subject verification method based on the trustees mechanism for remote registration”, Proceedings of TUSUR journal, vol. 3, issue 19, 2016, pp. 70-75 [“Metodika verifikacii lichnosti sub’ekta dostupa pri udalennoj registracii s pomoshch’yu doverennyh lic”, Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioehlektroniki, vol. 3, issue 19, 2016, pp. 70-75] (In Russian).

[7] H. Celikkanat, E. Sahin, “Steering self-organized robot flocks through externally guided individuals”, Neural Computing and Applications, vol. 19(6), 2010, pp. 849–865.

[8] M. Dorigo, M. Birattari, T. Stьtzle, “Ant colony optimization: Artificial ants as a computational intelligence technique”, IEEE Computational Intelligence Magazine, vol. 1, No. 4, 2006, pp. 28–39.

[9] I.A. Zikratov, E.V. Kozlova, T.V. Zikratova, “Vulnerability analysis of robotic systems with swarm intelligence”, Scientific and Technical Journal of Information Technologies, Mechanics and Optics, vol. 5 (87), 2013, pp. 149-154 [“Analiz uyazvimostej robototekhnicheskih kompleksov s roevym intellektom”, Nauchno-tekhnicheskij vestnik

informacionnyh tekhnologij, mekhaniki i optiki, vol. 5 (87), 2013, pp. 149-154] (In Russian).

[10] F. Higgins, A. Tomlinson, K.M. Martin, “Survey on security challenges for swarm robotics”, 2009 Fifth International Conference on Autonomic and Autonomous Systems, Los Alamitos, CA, USA, April 2009, pp. 307–312.

[11] I. Navarro, F. Matia, “An Introduction to Swarm Robotics”, International Scholarly Research Notices on Robotic, vol. 2013, 2013, acticle ID 608164.

[12] I. Navarro, F. Matia, “Survey of Collective Movement of Mobile Robots”, International Journal of Advanced Robotic Systems, vol. 10, issue 1, 2013.

[13] A.S. Sigov, V.V. Nechaev, V.V. Baranyuk, O.S. Smirnova, “Approaches to group control and information-driven interaction in heterogeneous robot squads”, Modern Information Technology and IT-education, vol. 1, 2016, pp. 146-151 [“Podhody k formirovaniyu edinogo informacionnogo-upravlyayushchego polya smeshannyh robototekhnicheskih gruppirovok”, Sovremennye informacionnye tekhnologii i IT-obrazovanie, vol. 1, 2016, pp. 146-151] (In Russian).

[14] P.A. Budko, A.M. Vinogradenko, A.I. Litvinov, “Reconfiguration of communication channels at management of mixed groups of robotic complexes”, Izvestiya SFedU. Engineering sciences, vol. 2 (187), 2017, pp. 266-278 [“Rekonfiguraciya kanalov svyazi pri upravlenii smeshannymi gruppirovkami robototekhnicheskih kompleksov”, Izvestiya YuFU. Tekhnicheskie nauki, vol. 2 (187), 2017, pp. 266-278] (In Russian).

[15] E.S. Basan, A.S. Basan, O.B. Makarevich, “Development and implementation of a method to detect an abnormal behavior of nodes in a group of robots”, Bezopasnost informacionnyh tehnology, vol. 25, no. 4 , 2018, pp.76-86 [“Razrabotka i realizaciya metoda obnaruzheniya anomal'nogo povedeniya uzlov v gruppe robotov", Bezopasnost informacionnyh tekhnologij, vol. 25, no. 4 , 2018, pp.76-86] (In Russian).

[16] O. Petrovsky, “Attack on the drones”, Proceedings of Virus bulletin conference, 2015, pp. 16-24.

[17] A.S. Basan, E.S. Basan, O.B. Makarevich, “The method of resistance to active attacks in wireless sensor networks”, Izvestiya SFedU. Engineering sciences, vol. 5 (190), 2017, pp. 16-25 [“Metod protivodejstviya aktivnym atakam zloumyshlennika v besprovodnyh sensornyh setyah”, Izvestiya YuFU. Tekhnicheskie nauki, vol. 5 (190), 2017, pp. 16-25] (In Russian).

[18] A.A. Sholokhova, A.N. Ivanov, “Dynamical systems modeling based on polynomial neural networks”, Scientific journal “Modeling, Optimization and Information Technology”, vol. 4(19), 2017 [“Modelirovanie dinamicheskih sistem na osnove polinomial'nyh nejronnyh setej”, Nauchnyj zhurnal “Modelirovanie, optimizaciya i informacionnye tekhnologii”, vol. 4(19), 2017] (In Russian).

[19] M. Shashanka, M. Shen, J. Wang, “User and entity behavior analytics for enterprise security” ,2016 IEEE International Conference on Big Data (Big Data), Washington, DC, 2016, pp. 1867-1874.