Modeling of information security system and automated assessment of the integrated quality of the impact of controls on the functional stability of the organizational system

© Babenko Tetiana[0000-0003-1184-9483], © Hryhorii Hnatiienko[0000-0002-0465-5018] and © Vialkova Vira[0000-0001-9109-0280]
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

babenkot@ua.fm, G.Gna5@ukr.net, veravialkova@gmail.com

Abstract. A mathematical model of the control system implementation problem is proposed. The concept of criticality of controls, as well as various aspects of functional stability and its relationship with reliability, survivability, fault tolerance are considered. Significant attention is paid to taking into account the subjective component in the tasks of determining the quality of implementation of controls and evaluation of the integrated security indicator of the information system. Attention is paid to the consideration of granularity in the construction of the function of belonging to a fuzzy set. The problem of assessing the integrated quality of control implementation and solving the optimization problem of improving the quality of information system security is considered.

Keywords: control system, information security, critical information infrastructure objects, functional stability, decision making, fuzzy set membership function.

1 Introduction

Reliable and, in some situations, sufficient protection of the information security management system is an important aspect of its existence and the subject of attention of a large number of specialists. Building a perfectly reliable system of information protection, processed using information and communication systems, is a fundamentally impossible task. In modern conditions, the measures and means of information protection used can only significantly reduce the likelihood of negative consequences of violation of the basic properties of information or damage from them, but do not allow to avoid them completely. Therefore, it makes sense to consider the process of ensuring information security at some acceptable level for the organization, which corresponds to the real threats.

The controls to be implemented when building an information security management system or when building information systems are described, in particular, in [1]. Some of the controls are extremely important for the functioning of the system. For the rest

of the controls, a reduced level of control implementation is allowed, and for some situations, even the absence of some controls is possible without significant danger to a sufficient level of functional stability of the system.

When building a control system in full accordance with the standard [2], the quality of all controls is one hundred percent and their set is equal to the set of all possible control indices. That is, such a situation is ideal and the distance from it to the actual existing control system, which is audited, can serve as a criterion for the quality of the built control system. In an ideal situation, all standards must be met. But achieving this level of control is too costly. In many practical situations, the level of information security has to be sacrificed to some extent. - Growing companies cannot afford to achieve such an expensive ideal. Therefore, a compromise is proposed - "best practices" as a guide.

2 Models for assessing the quality of information security services

The increased level of attention to the problems of assessing the security of information systems (IS) is explained, among other things, by the emergence of new forms of hostilities, including hybrid warfare, one of the goals of which is to disrupt critical information infrastructure (CII). As you know, the national security and defense of any state depend on the constant work of the CII. Analysis of open publications in the field of CII disruption and its consequences shows that such influence as a tool is quite common and can significantly weaken the position of the countries concerned in a particular area and in globalization is used as an element of political and economic pressure. The problem of CII security assessment is significantly complicated by the fact that CII entities have different forms of ownership and different requirements to ensure the protection of the basic properties of information processed in their IP and, accordingly, can use their own requirements to protect a wide range of frameworks and so-called "best practices", in particular such as NIST Cyber Security Framework (CSF), MITER ATT&CK Framework, NIST Framework for Improving Critical Infrastructure Cybersecurity, Control Objectives for Information and Related Technology (COBIT), NIST 800-53 v5, ISO 2700X, 1504 and others. [2-9] These regulations are recommended by their developers to use outside the United States in the commercial and public sectors [3, 4]. In this context, it should be noted that many countries, based on the relevant frameworks, will develop their own regulations and methodologies for the creation of protection systems, including at CII facilities.

Thus, in the sector of information security services processed at CII facilities, there is a wide variety of approaches to the implementation of information security systems and possible methods for assessing the level of CII security. Conformity analysis of information protection systems implemented on the basis of "best practices" and assessment of the level of security of CII objects is performed based on a risk-oriented approach, which allows to manage cyber security risks and, accordingly, improve the level of protection of CII objects. Risk in this context means a potentially possible event in the field of cybersecurity, which may lead to a violation of the basic properties of the

protected information. At the same time, it is also necessary to take into account the fact that the analysis must be performed at different stages of the life cycle of the CII object, which, in turn, sometimes requires processing significant amounts of unstructured data in conditions of uncertainty and time shortage and the probable use of destructive actions (methods and means of social engineering) against authorized CII users.

It is known that the construction and maintenance at a given level of information security systems or information security management systems (ISMS) at CII facilities requires a systematic approach to managing cybersecurity risks and identifying the needs of a particular organization in relation to information protection requirements. According to "best practices", it is considered that the process of cybersecurity risk management should be consistent with the overall risk management process of the enterprise and should be applied both in the process of creation and in the process of ISMS. According to [10], the process of cybersecurity risk management consists of identifying circumstances, assessing risks, processing risks, accepting risks, discussing risks and consulting, monitoring and reviewing risks. The process of risk processing should be cyclical and based on the results of the risk assessment of violation of the accepted level of guarantees to ensure the basic properties of information.

Assuming that the process of risk assessment and processing is one of the key to determining the current level of cybersecurity of CII facilities and the current effectiveness of ISMS and ways to achieve the target profile (Target Profile) for analysis and assessment of identified risks, use a qualitative or quantitative approach. The quantitative approach theoretically allows to compare the achieved level of maturity of the implemented ISMS, but its application in practice is complicated by the following factors [1, 11]:

- lack of reliable statistics;
- the difficulty of assessing losses in the case of intangible assets;
- the difficulty of assessing indirect losses from the implementation of threats;
- depreciation of the results of long-term quantitative risk assessment due to the modification of the ISMS.

Thus, the process of IS risk assessment is quite subjective, and its results significantly depend on the adopted assessment methodology, business objectives of the enterprise and the level of staff training that ensures the performance of external and internal audit of the CII. Existing tools for assessing the effectiveness of IP and within them ISMS, which is the result of the use of a "best practice" include models of maturity and models of process capabilities. As a rule, various tools for assessing the effectiveness of ISMS use a maturity assessment system, which scales from 0 to 5, and 5 is the highest level of maturity [12]:

0 - Not performed;
1 - Performed informally;
2 - Planned;
3 - Well defined;
4 - Quantitatively controlled;
5 - Continuous improvement.

In different implementations of this toolkit, there are differences in the methodology of application: as a rule, the assessment of the level of maturity of ISMS is carried out by an information security officer, consultant or auditor. The number of questions and the methodology for obtaining the resulting answer may differ depending on the maturity model for which of the "best practices" need to be determined (CMMI, NIST, COBIT, ISO 21827, etc.). In most cases, the assessment of the level of maturity focuses on the study of the following issues:

- what are the intentions of the organization to implement information security policy (ISO 5);
- how the organization manages its information security (ISO 6);
- whether staff are qualified to perform their duties and whether access to resources is terminated after their dismissal (ISO 7);
- whether the asset management program includes methods of identification, tracking, classification of property rights to assets for their protection (ISO 8);
- whether the organization uses administrative, physical, technical functions to manage the capabilities of users of IP and information and communication systems to interact with other information resources (ISO 9);
- how the organization uses cryptographic security methods and how cryptographic keys are managed (ISO 10);
- how buildings and related infrastructure are protected from IS threats (ISO 11);
- as formalized policies of procedures and controls that help ensure data and IP protection and assist in the management and operation of networks (ISO 12,13);
- whether security requirements are established in the organization as an integral part of the development or implementation of ISMS (ISO 14);
- how safe the organization is interaction with third parties (ISO 15);
- how IS incidents are managed (ISO 16);
- whether business continuity management is performed (ISO 17);
- whether compliance with legal requirements for the protection of information assets is ensured (ISO 18).

Studying such a wide range of issues without the involvement of external experts in the field of IS audit is, in most cases, a problem that has no solutions.

In case when the organization seeks to comply with any of the "best practices", it must ensure compliance with the relevant conditions of a particular "best practice" [1] and in the construction of ISMS to implement the relevant basic elements of information security management. Given the continuous improvement of "best practices", such as the need to meet new challenges of the time, the difference between versions of the same "best practice" may be significant, which will require significant modifications to existing ISMS and the corresponding costs of CII owners. often unwilling to carry. For example, the difference between the NIST 800-53 v4 and NIST 800-53 v5 versions is quite significant. In version 5, 66 new controls were added and 202 controls were improved, 131 new parameters were added to the existing controls. As a result of a number of improvements in NIST 800-53 v5, 1007 controls and improvements were created. In some best practices, in particular in the NIST CSF, it is stated that the core of the standard is widely related to controls from common international standards, such as ISO / IEC 27001, NIST 800-53, COBIT, Council on Cybersecurity (CCS), Critical

Security Controls (CSC), and the security standard for industrial automated systems and control systems ANSI / ISA-62443, and CII of real objects, as a rule, is heterogeneous and, accordingly, requires integration and analysis of complex solutions and significant costs for creation and modernization of existing SUIB.

Based on the fact that the creation or modernization of an existing ISMS requires significant investment, at the same time, excessive implementation of controls, with the exception of the economic component, increases the level of complexity and, consequently, reduces the reliability of ISMS complexity of staff support and dissatisfaction. Thus, to determine a sufficient level of controls implemented in the ISMS in accordance with specific "best practices" or their set, which would ensure the protection of information processed at CII facilities at a given level of guarantees at which the ratio of costs for security measures and the amount of possible losses should have a level acceptable to the organization is relevant.

The tasks of ensuring the functional stability of systems are constantly in the field of view of researchers [13, 14]. Many scientific papers today are also devoted to information security and critical cybersecurity infrastructure management [15, 16].

This work proposes a mathematical model that allows, based on a list of controls implemented in a particular ISMS, to determine the level of its reliability, in relation to the goals assigned to it by the owners of the CII or individual IP.

3 Formulation of the problem

In many practical situations, a significant part of domestic companies cannot afford the full-scale implementation of a complete and comprehensive information security system that would fully meet the relevant existing tasks and challenges. Therefore, in some cases, companies use as a guideline or example for the creation of ISMS so-called "best practices" that have proven themselves in real situations and can be implemented with less labor and financial costs, but provide a sufficient level of information security for a particular company.

Suppose that an information security management system is built, for which, in accordance with "best practice" [1, 7], a system of controls is defined and implemented. We will denote the set of control indices $i \in I = \{1,...,n\}$.

In this case, each control is characterized by the level of its implementation in the system $a_i, i \in I$, and the quality of its application or robustness $b_i, i \in I$, level of implementation $a_i, i \in I$, and quality $b_i, i \in I$. Without reducing the generality, we will assume that $0 \le a_i \le 1, \forall i \in I$ та $0 \le b_i \le 1, \forall i \in I$. The level and quality are determined by experts or using specially designed procedures.

Let the relationships between controls be known, evaluated or expertly determined $v_{ij}, i, j \in I$, which characterize the level of influence of control with the index *i*: $a_i, i \in I$, on control with the index *j*: $a_j, j \in I$. Without reducing the generality, we will also assume that $0 \le v_{ij} \le 1, \forall i, j \in I$.

The task is to model the characteristics of the information security management system (ISMS), which is created, as well as arithmetic (metrization, digitization) of quality controls and determine an integrated assessment of the level of information security. The ultimate goal of such modeling is to ensure the functional stability of the system [17]. For the task of providing information protection, the functional stability of the system is to determine such a configuration of controls and to choose such a limit level of quality of controls that allow to ensure an acceptable level of protection.

4 Mathematical model

The set of controls and relationships between them will be modeled by graphs or matrices of contiguity or incidence. Note that the level of control implementation can be characterized by some discrete values: scores, verbal expressions, clustered indicators, and so on. In any case, it should be emphasized that the measurement is performed on an ordinal scale. Therefore, the average in such cases should be defined as the median, not as an arithmetic mean. And the quality of control is functionally dependent on the level of its implementation and is expressed by some given or empirically defined function - in analytical or tabular terms $b_i = f(a_i), i \in I$.

Based on the analysis of controls, with the help of a group of experts, you can build a graph of the relationship of controls, which is generally multifaceted. The vertices of the graph are controls with multiple indices $i \in I$, each of which is characterized by the level of implementation of control in the system $a_i, i \in I$, and quality of operation $b_i, i \in I$. The relationships between the controls are graph arcs $v_{ij}, i, j \in I$. In the absence of an arc between some vertices of the graph under construction, i.e. $\exists : v_{ij} = 0, i, j \in I$, the impact of control with the index $i, i \in I$, on control with the index $j, j \in I$, is absent. The level of influence between controls is expressed in the feedback: positive and negative.

We will assume that at the initial stage of modeling and evaluation of ISMS it is determined that the level of implementation of controls in the system is $a_i^0, i \in I$, and the quality of functioning of each of them is defined or measured as. $b_i^0, i \in I$. The modeling of possible states of the system is that hypothetically or practically changes the initial levels of implementation of some controls and, according to the introduced heuristics, determines how these changes will affect the quality of interconnected controls and ISMS as a whole.

In this case, the level of influence between the controls is expressed in the feedback: this relationship can be positive or negative. Positive feedback $v_{ij}^+, i, j \in I$, is that in the case of reaching the top $i \in I$ of graph, even in the absence of control $a_i = 0, i \in I$, the system provides some level of quality at this peak, i.e. $b_i > 0, i \in I$. The specific numerical value of the level of quality control in this case is determined

by experts, experimentally, empirically or statistically. Negative feedback level $v_{ij}, i, j \in I$ when reducing the level of control $a_i^t < a_i^{t-1}, i \in I$, entails a decrease in the quality of control not only of this peak $b_i^t < b_i^{t-1}, i \in I$, but also the associated vertices of the graph: $b_j^t < b_j^{t-1}, \forall j : v_{ij} > 0, i, j \in I$, where $t-$ tact of quality assessment of the system: $t = 0,1,2,...$.

In the same way the interaction between the shares of the graph is modeled - through the bridges between the shares. We will also assume that in the case of a discontinuity of the graph, the modeling of each connectivity component can be performed autonomously, by analogy with the approach described in this paper.

The task is to maximize the integrated level of quality controls and minimize the cost of their implementation.

5 Model for determining the quality of performance of elements of the organizational system

Suppose that $i-$ element of the system is missing and subset problems $A^i, i \in J,$ executes an element with an index $j, \ j \in J,$ or several elements($k_i, k_i < k,$) with indeces $j_t \in J \setminus \{i\}, t = 1,..., k_i.$ Thus, according to the accepted heuristics, quality of performance of problems of a subset $A^i, i \in J,$ may be about 80% of the nominal. Due to the additional load on items with indexes $j_t \in J \setminus \{i\}, t = 1,..., k_i,$ the quality of subsets $A^{j_t}, j_t \in J, \ t \in J \setminus \{i\}, \ i \in J,$ will also decrease significantly.

Quality of performance of functions from subsets $A^i, i \in J,$ and $A^{j_t}, j_t \in J, \ t \in J \setminus \{i\}, \ i \in J,$ can be set in the described case also by membership functions $\mu_{ij}(x), i \in J, \ j \in J^i,$ where $x < 100\%, \ J^i -$ a set of indexes of functions belonging to a subset of functions of a particular system element $A^i, i \in J.$ Thus, with a significant additional load on the element of the system, which is transferred to perform the task of the missing element, significantly reduces not only the quality of new tasks, but also the tasks that he previously performed. This model should consider additional features.

In addition, in the situation of long-term absence of a system element there are additional costs:

- losses in duplicate execution of subtasks described by membership functions;
- the cost of time and resources to find and replace the missing element of the system (internal recruitment or implementation of technical regulations in technical systems);

- payment for external recruitment or involvement of external repair services in technical systems;
- the cost of time and resources of the entire system, depending on the probability of a successful search for a replacement item that is excluded from the system;
- the cost of the procedure of adaptation of a new element, the cost of interaction with adjacent interconnected elements (the effectiveness of this procedure and its duration can also be described by membership functions);
- when modeling the described situation should also take into account the duration of the new element in the system, the cost of such a set of tasks in the market and other factors.

6 Assessment of the integrated control level

Today there is a group of indicators that are used to determine the overall security of the system. One of the common tasks of expert evaluation is the choice in a pre-fixed class of relations of some resulting (group, collective, compromise) relationship. At the same time, on the basis of several contradictory indicators, the aggregation (aggregation, integration, generalization, etc.) of indicators into a single integrated indicator is carried out. To construct a convolution (generalized, aggregating, integral, integrative criterion of quality of object) - it means to supplement a partial order on set of objects to full. This procedure can be carried out in many ways and necessarily includes an element of subjectivity.

At the first stage, experts build a model of an ideal control system that meets the standard [2], in the form of a graph with normative vertices and arcs, the model of which is described above.

At the second stage, an expert or group of experts who audit the real control system and establish or assess the presence of controls, the level of their implementation in the system and fill in the column that simulates the real ISMS. The coefficients of relative competence of experts can be taken into account [18], etc.

On the basis of expertly determined or calculated by another method of control levels $a_i, i \in I$, considering the system that meets the standard [2], dependings on this information quality levels of control are determined: $b_i, i \in I$.

In the third stage, with the participation of experts, the quality levels of the ISMS are clustered to build an integrated membership function [19], which reflects the distribution of quality controls by quality levels and creates a membership function based on the frequency of values. The integral value of the level of quality of the implementation of the control system, which indicates the degree of functional stability of the system, can be calculated, for example, by the method developed by the authors [17].

To determine the integrated assessment, we build a matrix of frequencies of different levels of quality of performance functions $V = (v_{ij}), \; i = 1,...,100, \;\; j < n.$ Each row of this matrix displays the estimated level of function quality from 0% to 100%, and the column shows the number of functions with the specified level of performance.

To determine the integrated level of quality of functioning of a complex system, the classification of functions by the level of quality and completeness of their implementation is carried out. After that, the function of belonging to a fuzzy set of values of the integral quality of control implementation is constructed [17, 20].

The integral value of the quality level of the control system, which indicates the degree of functional stability of the system, can be calculated, for example, by the method described in [17]. An integrated assessment of the quality of the information security system will be determined using an additive criterion. In this case, we use a number of heuristics that allow to justify the adequacy of the calculation of a single integral value of the criterion.

The quality of the information security system largely depends on the quality of the system elements. Determining the integrated level of quality of a complex poorly structured system based on the analysis of the interchangeability of its subsystems and determining the best options for improving the quality of functions requires the creation of an appropriate mathematical model.

7 Optimization of the system protection integrated quality

To increase the overall (resulting, integrated, aggregate, integrative) level of quality of control system implementation, an expert or group of experts suggests options to improve the system quality by increasing the level of implementation of some controls and estimating the cost of implementing higher levels of individual controls. This is due to the limited resources that the organization can allocate to improve the quality of the information security management system. The task of choosing a compromise option to ensure quality control is a multifaceted problem and can be formalized in the classroom of multi-criteria optimization or by applying the idea of system optimization [21]. System optimization for the task of building an information security model is to determine the decision maker, the allowable level of protection and to optimize only those controls that are critical to ensure the level of protection of the system as a whole. It should be borne in mind that the definition of directions and the choice of options for optimizing the integrated level of information security of the organizational system is a multi-criteria task [22]. In addition to ensuring the desired level of implementation of controls, almost every organization should take into account, in particular, their financial capabilities.

Due to the computational complexity of the problem of direct search of control system optimization options, experts can suggest, for example, about ten such options to improve quality. There may also be comprehensive options when estimating or monitoring the cost of combined control improvements.

On the basis of the options offered by experts of increase of level of introduction of separate additional controls recalculation of new states of system is carried out. That is, the optimization two-criterion problem is solved to improve the integrated quality of the protection system and minimize the cost of improving the condition of individual controls. Scales and the admissibility of transactions with indicators play an important role.

8 Areas of further research

The problem described in this work has broad prospects for research and modeling of information security of a complex system. Based on the described approach, new problem statements can be developed and new approaches to improving the adequacy of modeling can be identified. To more fully take into account the features of real systems, it is necessary to complicate the described mathematical model. In particular, this can be done by taking into account the following factors:

- determination of the limits of reducing the margin of safety of the system, assessment of threats to its information security;
- assessment of the allowable level of reduction of information security of the system elements and the level of task performance;
- considering the presence or absence of links between tasks: the impact of the task on the quality of other tasks;
- solving optimization problems of forecasting the quality of the system, the cost of ensuring this quality and calculating the allowable time;
- restoration of the admissible level of quality of functioning of system at failure of several its elements: definition of necessary conditions of functioning.

It is also perspective to use the RACI methodology for the development of a matrix of responsibility distribution, which is used in various management doctrines: functional, process and design: Responsible, Accountable, Consult before doing, Inform after doing.

In further research, it is also possible to construct functions for a priori introduced linguistic variables with the following names: "critically acceptable level of information security", "risky operation of the system", "sufficient level of information security", "high level of information security" and so on.

9 Conclusions

A model for assessing the integrated quality of the information security management system and ways to purposefully improve the quality of its operation are proposed.

Also substantiated:

- Built model of controls;
- Admissibility of expert assessment;
- An approach to determining an integrated assessment of the quality of implemented controls is proposed.

This model can be adapted to the needs of a particular organization, as well as applied in other subject areas. The model is open to improvement and can easily be focused on dealing with fuzzy data.

Reference

1. Diogenes Y., Ozkaya E. D44 Cybersecurity: Attack and Defense Strategies / translated from English. D. A. Belikova. - M .: DMK Press, 2020 .-- 326 p

2. State standard of Ukraine ISO/IEC 27001:2015.
3. https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf
4. SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations CSRC (nist.gov)
5. https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf
6. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov)
7. State standard of Ukraine ISO/IEC 27002:2015 Information Technology. Methods of protection. Code of practices for information security measures (ISO/IEC 27002:2013; Cor 1:2014; IDT)
8. State standard of Ukraine ISO/IEC 27006:2015
9. State standard of Ukraine ISO/IEC 27005:2015
10. ISO/IEC 31000:2018 Risk management – Guidelines
11. Bondarev V.V. Security analysis and monitoring of computer networks. Methods and means. / - Moscow: publishing house MSTU im. N.E. Bauman, 2017 -225 ill.
12. ISO/IEC 21827:2008 Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)
13. Kravchenko Yu.V. The current camp and development of the theory of functional style / Yu. V. Kravchenko, S. A. Mikus // Model and information technologies: collection of scientific practices IPME im. G.Є. Pukhova. - 2013. - VIP. 68. P. 60-68.
14. Kravchenko, Y., Vialkova, V. The problem of providing functional stability properties of information security systems // Modern Problems of Radio Engineering, Telecommunications and Computer Science, Proceedings of the 13th International Conference on TCSET 2016, 2016, pp. 526–530.
15. Toliupa, S., Parkhomenko, I., & Shvedova, H. Security and regulatory aspects of the critical infrastructure objects functioning and cyberpower level assesment. In 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings (pp. 463–468).
16. Slipachuk, L., Toliupa, S., & Nakonechnyi, V. The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine. In 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings (pp. 451–454).
17. Hnatiienko H., Vialkova V. Model-Based Analysis Of The Estimation Of Integral Level Of Secuhity Of The Information System // Scientific and Practical Cyber Security Journal (SPCSJ). Vol.2, No.4, December, 2018. Pp. 95-103.
18. Hnatiienko H., Snytyuk V. A posteriori determination of expert competence under uncertainty / Selected Papers of the XIX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2019), pp. 82–99 (2019).
19. N. Kiktev, V. Osypenko, N. Shkurpela, A. Balaniuk. Input Data Clustering for the Efficient Operation of Renewable Energy Sources in a Distributed Information System. 2020 IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT). 23-26 Sept. 2020, Zbarazh, Ukraine. pp. 9-12.
20. Hnatiienko H., Snytyuk V. Expert technologies accepted solutions: Monograph. - K .: LLS "Maklaut", 2008. - 444s.
21. Glushkov V. Fundamentals of paperless computer science. M.: Science. The main edition of physical and mathematical literature, 1982. - 552 p.
22. N. Kiktev, H. Rozorinov, M. Masoud. Information model of traction ability analysis of underground conveyors drives. 2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH). 20-23 April 2017, Lviv. pp. 143-145.