MODELS AND METHODS FOR ASSESSING THE SECURITY OF MULTI-FACTOR AUTHENTICATION MECHANISMS (p. 4-10)

Yuri Gorbenko, Inna Oleshko

Today many foreign companies rely on the protection methods, based on the mechanisms of multi-factor authentication. At the same time, the statistics of break-ins of the systems, using multi-factor authentication, is absent or negligible now.

The paper suggests the models for assessing the security of mechanisms of multi-factor authentication against unauthorized access, based on the calculation of probabilities of correct operation of authentication mechanisms and probabilities of unauthorized access.

Password protection systems, mechanisms based on the biometric characteristics and asymmetric cryptographic transformations are proposed to use as the main factors of multi-factor authentication system. As an example, the three-factor mechanism is considered, for which the model for assessing the security against unauthorized access is proposed.

Special cases of assessing security against unauthorized access are considered, when password protection mechanisms, biometric features and asymmetric cryptographic transformations are used as factors. The asymmetric cryptographic transformations are reviewed and analyzed according to the criteria of stability and complexity, recommendations for their practical use are given. Transformations in rings, finite fields, groups of points on elliptic curves and factor rings are proposed as the main cryptographic transformations that can be applied. The obtained results confirmed the possibility to implement multi-factor authentication method and allowed assessing its security against unauthorized access

Keywords: unauthorized access, multi-factor authentication, password protection mechanism, biometric characteristics, personal key

References

1. ISO/IEC 27032:2012(E). (2012). Information technology – Security techniques – Guidelines for cybersecurity. G.: ISO copyright office, 50.
2. Perlroth, N., Larson, J., Shane, S. (2013). N.S.A. Able to Foil Basic Safeguards of Privacy on Web. Newspaper The New York Times. Mode of access: http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html.
3. Proposal for a regulation of the european parliament and of the council on electronic identification and trust services for electronic transactions in the internal market. (2012). Brussels: Europian Commission, 119.
4. Schneier, B. (2002) Applied Cryptography. Protocols, Algorithms and Source Code in C. Moscow: Triumf, 816.
5. Stallings, W. (2001). Network and internet work security: principles and practice. Second Edition, Prentice-Hall, Inc., 672.
6. Gorbenko, I. D., Gorbenko, U. I. (2012). Applied cryptology. KNURE. Kharkov: Fort, 868.
7. Gorbenko, U. I., Gorbenko, I. D. (2010). Public Key Infrastructure. Electronic signature systems. Theory and practice. Kharkov: Fort, 593.
8. Simmons, G. J. (1984). Authentication Theory / Coding Theory. CRYPTO 1984, 411 – 431.
9. ISO/IEC 9798-1 (2010). Information technology – Security techniques – Entity authentication – Part 1: General. G.: ISO copyright office, 11.
10. DSTU 4145-2002. (2002). Information technology. Security techniques. Digital signature based on elliptic curves. Generation and verification. Kiev: Gospotrebstandart, 38.
11. DSTU ISO/IEC 9798-3-2002. (2005). Information technology. Security techniques. Entity authentication. – Part 3: Authentication SASL Mechanism. Kiev: Gospotrebstandart, 17.
12. Gorbenko, I. D., Oleshko, I.V. (2012). Method of assessment of relative entropy and comparative analysis of biometric information sources. Applied Radio Electronics: Sci. mag. Vol. 11, № 2, 255-261.
13. ISO/IEC 11770-3:2008. (2008). Information technology. Security techniques. Key management mechanisms using asymmetric techniques. G.: BSI, 94.
14. ISO/IEC 9797-1. (2011). Information technology – Security techniques – Message Authentication Codes (MACs). Mechanisms using a block cipher. G.: BSI, 52.
15. ISO/IEC 9797-2. (2011). Information technology. Security techniques. Message Authentication Codes (MACs). Mechanisms using a dedicated hashfunction. G.: BSI, 50.
16. ISO/IEC 14888-3:2006. (2006). Information technology. Security techniques. Digital signatures with appendix. Discrete logarithm based mechanisms. G.: BSI, 114.
17. ISO/IEC 9796-3:2006. (2006). Information technology. Security techniques. Digital signature schemes giving message recovery. Discrete logarithm based mechanisms. G.: BSI, 80.
18. ANSI X9. 98 – 2010. (2010). Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry. NY: ASME, 297.
19. Abe, M., Okamoto, T. (1999). A signature scheme with message recovery as secure as discrete logarithm. Advances in Cryptology - Asiacrypt 1999, Lecture notes in computer science. B.: Springer-Verlag, 378-389.
20. Maier, W., Staffelbach, O. (1988). Fast correlation attacks on certain stream ciphers. Journal of Cryptology. Volume 1, Issue 3, 159-176.

EVOLUTIONARY METHOD OF FACTOR ANALYSIS OF DATA PRESENTED IN THE FORM OF TRANSACTION DATABASES (p. 11-15)

Tatyana Zayko, Andrii Oliinyk, Sergey Subbotin

The solution of the problem of factor analysis automation in the diagnosis and recognition of images is considered in the paper, and some results of our research in this area are given.

The main purpose of the study is to develop an evolutionary method of factor analysis to find hidden dependencies in transactional databases. The use of modern methods of evolutionary search allows forming the groups of similar features.

The issues of extracting factor groups from the specified transactional databases are considered in the paper for identifying new knowledge when solving the problems of diagnosis and recognition of images.

The proposed method allows extracting the groups of qualitatively similar features from transactional databases. We propose to use the association rules to assess the equivalence of features terms that allows assessing the closeness of relationship between various features, making no demands to the input data and performing the factor analysis in

transactional databases. The research results can be used by researchers dealing with the study and analysis of complex objects, processes and systems with the purpose to identify new knowledge, as well as in decision support systems for technical and medical diagnostics

Keywords: association rule, rules database, feature, transaction, evolutionary search

References

1. Dopico, J. R., Calle, J. D., Sierra, A. P. (2009). Encyclopedia of artificial intelligence. New York : Information Science Reference, 1677.
2. Zajchenko, Ju. P. (2004). Osnovi proektuvannja intelektualnih sistem. Kyiv : Slovo, 352.
3. Boguslaev, A. V., Oliinyk, O. O, Oliinyk, A. O., Pavlenko, D. V., Subbotin, S. A. (2009). Progressivnye tehnologii modelirovanija, optimizacii i intellektualnoj avtomatizacii jetapov zhiznennogo cikla aviadvigatelej : monografija. Zaporozhe : Motor Sich, 468.
4. Jolliffe, I. T. (2002). Principal Component Analysis. Berlin : Springer-Verlag, 489.
5. Rummel, R. J. (1988). Applied Factor Analysis. Evanston : Northwestern University Press, 617.
6. Iberla, K. (1980). Faktornyj analiz. Moscow : Statistika, 398.
7. McLachlan, G. (2004). Discriminant Analysis and Statistical Pattern Recognition. New Jersey : John Wiley & Sons, 526.
8. Subbotin, S. O. (2008). Podannja j obrobka znan' u sistemah shtuchnogo intelektu ta pidtrimki prijnjattja rishen. Zaporizhzhja : ZNTU, 341.
9. Gkoulalas-Divanis, A., Verykios, V. S. (2010). Association Rule Hiding for Data Mining. New York: Springer-Verlag, 150.
10. Zhang, C., Zhang, S. (2002). Association rule mining: models and algorithms. Berlin : Springer-Verlag, 238.
11. Chambers, L. D. (2000). The Practical Handbook of Genetic Algorithms. Florida: CRC Press, 520.
12. Subbotin, S. O., Oliinyk, A. O., Oliinyk, O. O. (2009). Neiterativni, evoljucijni ta multiagentni metodi sintezu nechitkologichnih i nejromerezhnih modelej. Zaporizhzhja : ZNTU, 375.
13. Haupt, R. Haupt, S. (2004). Practical Genetic Algorithms. New Jersey: John Wiley & Sons, 261.
14. Zhao, Y., Zhang, C., Cao, L. (2009). Post-mining of association rules: techniques for effective knowledge extraction. New York: Information Science Reference, 372.

INFORMATION TECHNOLOGY OF CONSTRUCTION OF NEUROSIMULATOR OF SECURITY SYSTEMS ASSESSMENT (p. 16-21)

Igor Pilkevich, Nadya Lobanchikova, Volodimir Kotkov, Tatyana Kotkova

The use of modern information technologies can facilitate information processing and automate decision-making processes of experts in information security. The aim of the research is to develop the information technology of predicting the reliability of information security system activation for the automation of information security experts' work. The object of the study is the process of constructing intelligent systems of analysis and decision support.

The subjects of the study are models, methods and tools for building the intelligent systems of analysis and decision support in order to predict the reliability of security systems activation, automation of information processing by experts.

The information technology of development and implementation of the neurosimulator for predicting the reliability assessment of security systems and automation of the information security expert's work in order to minimize the time for data processing and decision-making is described in the paper.

The information technology can be used to predict a wide range of problems. The advantage of the proposed technology is the use of several variants of the activation function and network training methods, which allows to obtain a set of data for a thorough analysis and increase the objectivity of decision-making

Keywords: prediction, security, information, neuron, network, neurosimulator, classification, algorithm, training

References

1. Chen, P. P. (1976). The Entity-Relationship Model: Toward a Unified View of Data. ACM Trans. On Database Syst., V.1, №1, 9–36.
2. Codd, E. F. (1970). A relational model of data large shared data banks. Comm. ACM, V.13, №6, 377–387.
3. Glushkov, V. M. (1957). The structure of locally bicompact groups and fifth Hilbert's problem. Uspekhi matematicheskikh nauk, №12, 2(74), 3–41.
4. Palagin, A. V., Kryvyi, S. L., Petrenko, N. G. (2012). Ontological methods and means of processing of subject knowledge: monograph. Lugansk: VNU, 323.
5. Korchenko, O. G. (2004). Systems of priv: monograph. Kyiv: NAU, 264.
6. Subbotin, S. O. (2008). Knowledge presentation and processing in systems of artificial intelligence and decision support: textbook. manual. Zaporozhye: ZNTU, 341.
7. Gladun, V. P.,Velichko, V. Yu. (2012). Instrumental complex decision support based on the network model of the subject area. A decision support system. Theory and practice. Kyiv: IPMMS NANU, 126–128.
8. Ossovskii, S. (2002). Neural networks for information processing. Moscow: Finance and statistics, 344.
9. Gribunin, V. G., Chudovsky, V. V. (2009). Complex system of priv on an enterprise: train aid for the students of higher educational establishments. Moscow: Academy, 416.
10. Rutkovskaia, D., Pilinskii, M., Rutkovskii, L. (2007). Neural networks, genetic algorithms and fuzzy systems. Moscow: Hot line-Telecom, 452.

CONTEXTUAL SEARCH METHOD BASED ON THE THESAURUS OF KNOWLEDGE DOMAIN (p. 22-27)

Vasyl Lytvyn, Olha Moroz

The creation of the intellectual search engine was reviewed based on the domain thesaurus. Text linguistics was taken as the example of domain.

The approach to the creation of semantic metrics was suggested based on such a thesaurus. For this aim the weights of importances of the groups relations were introduced between the thesaurus terms (synonyms, correlates, holonyms, meronyms, hyperonyms).

The thesaurus was converted into the weighted conceptual graph. Based on Floyd-Warshall algorithm the distances between the terms of weighted conceptual graph were found. Those distances were used during the intellectual search of relevant text documents based on the key words. If some key words are not mentioned in the text document, the search engine looks for the most related term to the searched one. The efficiency of the proposed approach was introduced in comparison to other methods

Keywords: thesaurus; semantic metrics; intelligent search engine

References

1. Gladun A. J., Rogushina Y. V. (2007). Formation of the thesaurus as a means of modeling the information needs of the user when searching online. Bulletin of the computer. and Inform. technology, 1, 26-33.

2. Gruber T. A (1993). Translation approach to portable ontologies. Knowledge Acquisition, 5(2), 199-220.
3. Gavrilova T. A., Horoshevsky V. F. (2001). Knowledge base of intelligent systems. St. Petersburg: Peter, 384.
4. Strube M., Ponzetto S. (2006). WikiRelate! Computing semantic relatedness using Wikipedia. In Proceedings of the 21st National Conference on Artificial Intelligence,(AAAI 06). Boston, Mass., July 16-20, Mode of access: http://www.eml-research.de/english/research/nlp/public
5. Jarmasz M., Szpakowicz S. (2003). Roget's Thesaurus and semantic similarity. In Proceedings of Conference on Recent Advances in Natural Language Processing. Borovets, Bulgaria, 212-219.
6. Fellbaum C. (1998). WordNet: an electronic lexical database. MIT Press, Cambridge, Massachusetts, 423.
7. Wu Z., Palmer M. (1994). Verb semantics and lexical selection. In Proc. of ACL- 94, 133-138.
8. Resnik P. (1995). Disambiguating noun groupings with respect to WordNet. In Proceedings of the 3rd Workshop on Very Large Corpora. MIT, June, Mode of access : http://xxx.lanl.gov/abs/cmp-lg/9511006.
9. Resnik P. (1999). Semantic similarity in a taxonomy: an information-based measure and its application to problems of ambiguity in natural language. Journal of Artificial Intelligence Research (JAIR), Vol. 11, 95-130.
10. Lin D. (1998). An information-theoretic definition of similarity. In Proceedings of International Conference on Machine Learning, Madison, Wisconsin, July, Mode of access : http://www.cs.ualberta.ca/ ~ lindek / papers.htm
11. Smirnov A. V., Pashkin M. P., Shilov N. G., Levashova T. V. (2002). Ontology in artificial intelligence systems: methods of construction and organization. News of artificial intelligence, Moscow: Publishing House of the RAAI, 2, 3-9.
12. Sovpel I. V. (2004). The automatic extraction of knowledge from text and its applications. Scientific-theor. journal Artificial Intelligence, 3, 668-677.
13. Wu Z., Palmer M. (1994). Verb semantics and lexical selection. In Proc. of ACL- 94, 133-138.
14. Nikitin S. E. (1978). Thesaurus on Theoretical and Applied Linguistics. Moscow, USSR: Nauka, 220.
15. Lytvyn V., Shakhovska N., Pasichnyk V., Dosyn D. (2012). Searching the Relevant Precedents in Dataspaces Based on Adaptive Ontology. Computational Problems of Electrical Engineering, 2(1), 75-81.
16. Dosyn D., Lytvyn V. (2012). Planning of Intelligent Diagnostics Systems Based Domain Ontology. The VIIIth International Conference Perspective Technologies and Methods in MEMS Design, Polyana, Ukraine, 103.
17. Lytvyn V., Dosyn D., Medykovskyj M., Shakhovska N. (2011). Intelligent agent on the basis of adaptive ontologies construction. Signal Modelling Control, Lodz.
18. Swami M., Thulasiraman K. (1984). Graphs, Networks and Algorithms. Moscow: Nauka, 256.
19. Montes-y-Gómez M., Gelbukh A., López-López A. (2000) Comparison of Conceptual Graphs. Lecture Notes in Artificial Intelligence, 1793, Springer-Verlag: http://ccc.inaoep.mx/ ~ mmontesg / publicaciones / 2000/ComparisonCG.
20. Knappe R., Bulskov H., Andreasen T. (2004). Perspectives on Ontology-based Querying. International Journal of Intelligent Systems, http://akira.ruc.dk/ ~ knappe/publications/ijis2004.pdf.
21. Lytvyn V. (2013). Design of intelligent decision support systems using ontological approach. An international quarterly journal on economics in technology, new technologies and modelling processes, 2(1), 31-38.

FEATURES OF DEVELOPMENT OF SOFTWARE FOR THE DESIGN OF CONCRETE COMPOSITION

(p. 27-31)

Natalia Sizova, Ivan Mikheev

The methods for solving the problem of concrete composition design of various research schools of materials science in Ukraine: Rovno, Odessa, Kharkov schools are considered. The feasibility of application of information technologies for the formalization of various methods of concrete composition design is noted. The logical structure of intelligence decision-support system, which includes the information blocks and functional relations between them, is given. The functional requirements to the software, solving such problems were stated. These are simple interface, reasonable requirements to the hardware, reliability and safety, efficiency, user support. The fulfillment of the requirements is justified from the point of view of the possibility of software operation in the laboratory industrial conditions for the solution of the research and production tasks. The software user interface is given, primary and secondary problems are defined, which are solved using the information system

Keywords: concrete technology, concrete composition design, information technologies, intelligence systems

References

1. Latorec, K. V., Mikheev, I. A. (2011) Analysis of the application of modern information technology to address the production of concrete. Eastern-European Journal of enterprise technologies, 2/6 (50), pp. 32-34.
2. Actual problems of physicochemical Materials (2013). Donetsk, Ukraine. Nord Computer, 132.
3. Mikheev, I. A. (2011). Certificate of authorship № 39817 UA. Computer program «Concrete Design». Publ. 30.08.2011.
4. NIIZHB (1979). Manual selection of heavy concrete compositions. Moscow, USSR. Stroyizdat, 102.
5. Dvorkin, O. L. (2001). Multivariable design of concrete compositions. Rovno, Ukraine. RGTU, 121.
6. Dvorkin, L. I., Shamban, I. B. (1992) Multivariable prediction of the properties and design of concrete compositions. Moscow, Russia. Stroyizdat, 132.
7. Voznesensky, V. A. (1981) Statistical methods of experiment planning in feasibility studies. Moscow, USSR. Finance and Statistics, 263.
8. Voznesensky, V. A., Lyashenko, T. V., Ogarkov, B. L. (1989) Numerical methods for solving construction and technological problems on a computer. Kiev, USSR, High School, 328.
9. Plugin, M. A., Kalinin, O. A., Miroshnichenko, S. V., Plugin A. A. and others (2005) The method of determining the composition of ductile, trischynostiykoho and water impermeable concrete. Pat. UA 62613 Ukraine. IPC 7S04V28/12, Appl. 15.04.03, publ. 15.06.05, Bull. № 6.
10. Latorec, K. V., Mikheev, I. A. (2011) Analysis of modern design methods of concrete. Kharkiv, Ukraine. Scientific bulletin of construction, 63. 204-209.

ALGORITHMIC MODEL OF DISTRIBUTED SIMULATION PROCESS FOR TECHNOLOGY OF DISTRIBUTED SIMULATION MODELS ANALYSIS

(p. 32-36)

Maksym Volk, Rastislav Gridel, Cergej Sarancha, Denis Gavrish

Despite the widespread use of the distributed simulation, little attention has been paid to the construction of effective models of the distributed simulation itself and based on them analysis of the task flows in the systems of the cloud computing level with the purpose of obtaining the parameters and characteristics, used in task planners, resource brokers, scheduling algorithms.

The algorithmic model for the distributed simulation process, providing the extended set of the key parameters of the model is first proposed in the paper.

The model is based on the software representation of the simulation environment of modeling in the form of the set of executable code (activities of the particular model) and data (internal and external parameters, environment variables, data flows between particular models).

The proposed model first considers the actual time, taken for the performance of particular models, dynamic memory capacity in the course of experiments, idle time of resources and other parameters.

It is shown that on the basis of the proposed algorithm, it is possible to create a number of methods for the analysis of the distributed simulation models, the set of which allows to develop new technology of the analysis of the distributed simulation models.

The obtained results can be used in modern information technologies of the distributed simulation, in particular for the construction of the subsystem of distribution and dynamic redistribution of computing resources

Keywords: distributed simulation, algorithmic model, technology of analysis

References

1. Tomaszewski , B., Zhdanov E. (2003). Simulation modeling environment GPSS. - M.: Bestseller, 416p.
2. Yuditskii, S.A., Mouradian, I.A. (2007). Analysis Method configurations organizational systems on Petri nets // MBS, № 16, P. 163 -170.
3. Crane, M., Lemoine, A. Introduction to the regenerative method for analyzing models. Moscow: Nauka, 104p.
4. Okolnishnikov V.V. (2006). Development of tools for distributed simulation of multiprocessor computer systems. The dissertation of Dr. tehn. Sciences: 05.13.18. Novosibirsk, 227p.
5. Mitra, D., Mitrani I. (1984) Analysis and optimum performance of two message-passing parallel processors synchronized by rollback. Performance'84, pp.35-50.
6. Vosnesenskaya T.V. (2001). Mathematical model of time synchronization algorithms for distributed simulation . Software systems and tools . Thematic collection of CMC MSU faculty n. Lomomosov , pp. 56 -66.
7. Vosnesenskaya T.V. (2002). A mathematical model for analyzing the performance of distributed simulation systems. Artificial Intelligence (Donetsk), №2, pp. 74 -78.
8. Mics, A.I. Zamyatin E.B., Kozlov A.A. (2009). Software optimization of distributed simulation experiment. Scientific Service in the Internet: scalability , parallelism, efficiency : Proceedings of the All-Russian Supercomputer Conference (September 21-26, 2009, Novorossiysk), p. 524.
9. Ladyzhensky, Y.V. , Popoff Y.V. (2005). Software system for event-driven logic simulation. IEEE EWDWT, Odessa, September 15-19, 2005 , p. 119-122.
10. Ladyzhenskii Y.V Teslenko G.A. (2008). Mathematical model of the dynamic algorithm for distributed time progresses logic simulation of digital systems. Scientific works of Donetsk national technical university. Seriya: Informatics, cybernetics and computer engineering. - Donetsk, 2008 , № 9, p. 55-62.
11. Volk M.A. (2010). Analysis of distributed simulation models in heterogeneous computing systems Scientific Bulletin of Chernivtsi National University, handicrafts. Series: Computer systems and components, Volume 1, Issue 2, Chernivtsi, pp.35 -39.
12. Volk, M.A., Filimonchuk M.A., Al Shiblak M., Gridel R.N. (2012). Analysis of distributed simulation models with conservative synchronization algorithms. Collection of Sciences HUPS, 2012, V. 1 (30), pp. 95-98.
13. Volk, M.A., Al Shiblak, M., Gridel, R.N. (2013). Analysis of distributed simulation models with optimistic synchronization algorithms. Information processing system, 2013, V. 1(108), pp.35 -40.

A PROGRAMMABLE LOGIC CONTROLLER AS AN INDUSTRIAL OBJECT EMULATOR (p. 37-41)

Oleksandr Dobrzhanskyi

The results of the research are given in the paper, the main purpose of which is the development of the emulator of industrial objects, which is characterized by portability, versatility on a reproduction of transfer functions of typical control objects, support of standard configurations of input/output signals, support of the possibility of remote control and readjustment. Using the modern hardware provided by the scientific and production association «Owen» for research conducting and the software platform CoDeSys, a portable and flexible in the readjustment industrial object emulator was developed based on the controller PLC100-RL. The functional diagram of connection of such an emulator to the mounted automated control system is given. The structures of programs for the reproduction of basic transfer functions of typical industrial objects are proposed. The process of setting the configuration of input and output channels of the emulator was considered in details.

Flexibility of readjustment is provided by the possibility of reprogramming, and universality – by the presence of discrete and analog inputs/outputs, with standard signal levels 0- 20mA, 0- 1V. The Ethernet interface allows remote control and readjustment. For complex and distributed objects it is possible to complicate the emulator by the cascade inclusion of individual controllers-emulators.

The proposed methods and approaches extend the range of the use of network technologies and programmable logic controllers, namely they can be used for improvement of performance and expansion of the functionality of existing emulators of industrial objects, simplification and cost reduction of the stage of adjusting the systems of automated control of industrial processes

Keywords: emulator, automation, synthesis, controller, adjustment, program, configuration

References

1. Feldbaum, A. A. (1971). The Automatic Control Theory Methods. Moscow, USSR: Science, 744.
2. Kogan, B. Y. (1963). Electronic Simulators and Their Applications in the Research of the Automatic Control Systems. Moscow, PhysMathChiefPabl, 132.
3. Kasik, V., Jahan, S., & Kurecka, A. "FPGA Based Digital Logic Emulator for Educational Purposes," in Proc. 2011 International Conference on Software and Computer Applications, Singapore, 2011, 23-27.
4. Maslov, A., & Viskov, F. (2001). The Aggregate Equipment for Design and Adjusting Pojects of the Industrial Automatic Control Systems. Modern Control Technologies, Vol.9, 68-76.
5. Syzrantsev, V. N., Gammer, M. D., & Cherezov, K. M. (2006). Computer Simulators in Students' Training for oil-gas Sector of Industry. Drilling and Oil, 10, 34-36.
6. Okolnishnikov, V. (2011). Development of process control systems with the use of emulation models. International Journal of Mathematics and Computers in Simulation, Issue 6, Volume 5, 553-560.
7. Zakvasov, V. V., Perekrest, A. L., Gorbatko, S. V., Zakvasova, S. V., & Zamariev, G. V. (2010). Complex of hardware and software for the research of the discrete process of industry (physical structure and virtual model). Journal of KSUniv named after Mykhailo Ostrohratskyi, 4(63)-3, 172-175.
8. Papinov, V. M. "Hybrid model of automated process control systems-based computerized stands," in Proc. of 13 International Conference on Automated Control - Automatic-2006, Vinnytsia, 2006, 467.
9. Fernandez-Samaca, L., Ramirez Scarpetta, J. M., & Orozco-Guitierrez, M. L. (2010). Emulation and remote experimentation as support resources in a PBL approach for control systems. Rev. Fac. Ing. Univ., № 55, 194-202.
10. Ramirez, J., Caicedo, E. L., Pinedo, C., Bacca, E., & Ramos C. "A platform for signals and systems internet-based education," in Proc. Inted conference, Valencia, 2008, 1-8.

OPTIMIZATION OF MANAGING MULTIDIMENSIONAL PROCESS OF SINGLE-CRYSTAL GROWTH (p. 41-45)

Victor Suzdal, Yuriy Yepifanov, Igor Tawrovsky

The use of opportunities of systems of non-adaptive control, in particular, modal for high-quality management of linear dynamic objects is considered, and some results of our research in this field are given in the paper. The main objective of the research is to solve the problem of synthesis of stabilization law for a multidimensional control object based on the use of knowledge in the field of management, obtained from various sources, for the technological process of single-crystal growing by the Chokhralsky method on "GROWTH" setups. Current methods and means of ensuring the specified requirements to the management process imply distribution of matrix eigenvalues or transfer matrixes of a closed-loop system in the given points and areas, optimization of transients in the closed-loop system.

The methods for stabilization of a condition of multidimensional object using the system, providing the implementation of the specified requirements to the management process on the basis of decomposition of the model of the growth process as a control object, are considered in the paper. The proposed method with the use of graphic representation of the sensitivity function for the analysis allows to obtain important information on high-quality management of the system for the obtained matrix components of this system.

The algorithm of choosing the most appropriate matrix components for the model of the particular control object is presented. We propose to use this method for the increase in the accuracy of maintaining thermal conditions of the crystal growth, both in the stationary environment, and at the maximum perturbations of modes, with the purpose of improving the efficiency of management systems by modern growth setups in conditions of producing these single-crystals.

The research results can be applied by specialists in the field of robust modal management of material, energetic and informational flows in the systems of management of modern technological processes, introduced into the technical environment of these technological processes

Keywords: single-crystal, growth, management, optimization, system, model, decomposition, quality, stability

References

1. Goriletsky, V., Grinev, B., Zaslavsky, B. at all. (2002). Rost kristallov. Kharkov : AKTA, 535.
2. Kalman, R. (1960). Contributions to the theory of optimal control. Bulletin de la Sociedad Matematica Mexicana, 5, 102–119.

3. Wonham, W. (1967). On pole-assignment in multi-input controllable systems. IEEE Trans. Automat. Control, 12, 660–667.
4. Skelton, R., Iwasaki, T., & Grigoriadis, K. (1998). An unified algebraic approach to linear control design. L : Taylor & Francis Ltd.
5. Chilali, M., Gahinet, P. (1996). H∞ design with pole placement constraints: an LMI approach. IEEE Trans. Automat. Control, 41, pp. 358–367.
6. Scherer, C., Gahinet, P., & Chilali M. (1997). Multiobjective output-feedback control via LMI optimization. IEEE Trans. Automat. Control, 42, 896–911.
7. Mcfarlane, D., Glover, K. (1992). Loop shaping design procedure using H∞ synthesis. IEEE Trans. on Automat. Control, 37, 759–769.
8. Kailath, T. (1980). Linear systems. Englewood cliffs. NJ : Prentice Hall.
9. Iracleous, D., Alexandridis, F. (1999). A simple solution to the optimal eigenvalue assignment problem. IEEE Trans. Automat. Control, 44, 1746–1749.
10. Zubov, N., Mikrin, E., Negodyaev, S., Ryabchenko, V., Lapin, A. (2012). Optimizatsiya zakonov upravleniya orbitalnoy stabilizatsii kosmicheskogo apparata. M : MFTI WORKS, 4, 164–176.
11. Suzdal, V., Yepifanov, Y., Sobolev, A., Tawrovsky, I. (2009). Parametricheskaya identifikatsiya VARMAX modeley protsessa kristallizatsiyi krupnogabaritnykh monokristallov. Novi tekhnologiyi: Kremenchug, 4 (26), 23–29.

THEORETICAL STUDIES OF THE SPECIALIZED SYSTEM OF AUTOMATED CONTROL AND MANAGEMENT OF ELECTRICALLY HEATED FLOOR

(p. 46-52)

Nickolay Romanchenko, Anatoliy Slesarenko

The results of the study of the system of automated control and management of the operating mode of specialized electric heaters of the tubular type, which are the part of the power heat-generating modules of electrically heated floor in technologically active areas of livestock production facilities of various functional purposes, are presented. The automated control system for the multilayer electric-heat-accumulating heating system of production livestock facilities was studied, which operates under the "bottom-up" scheme and allows more accurate and energy efficient observance of the set temperature mode of the electrically heated floor surface, significant reduction of the expenditure of energy carriers and fodder resources in the processes of livestock production, reduction of the negative impact of livestock production waste on the environment and improvement of production standards in the industry. The proposed automated electrotechnical complex for the use in the systems of agricultural production livestock facilities with electrically heated floors allows more efficient use of energy, fodder and investment resources in the manufacture of high-quality competitive livestock products, improvement of production standards in the industry and reduction of the negative impact of production waste on the environment. The proposed automated system of MEHHS in comparison with existing heating systems of AIC facilities allows efficient operation under the "center-periphery" scheme in technologically safe and sustainable mode that in turn allows real-time remote control of thermal parameters of microclimate of the n-number of PLF in the large area from the single center using modern communication means

Keywords: energy efficiency, environmental compatibility, microclimate, electric-heat-accumulation, automation, economic efficiency

References

1. Krukovskij, P. G. Timchenko, N. P., Sudak, O. Ju (2002). Teplovye rezhimy polov razlichnyh konstrukcij s jelektrokabel'nymi sistemami obogreva. Promyshl. teplotehn, T. 24, №1, 10 - 16.
2. Romanchenko, M. A., Slesarenko, A. P., Soroka, O. S., Rumjancev, O. O. Pat. 63667A UA, MKI A 01 K 1/015. Ustanovka dlja zabezpechennja teplovogo rezhimu virobnichih primishhen' i sporud (UA). №2003054650; issued 22.05.2003; Opubl. 15.01.2004; Bjul. №1, 2
3. Engineering manual of automatic control for commercial buildings (1997). Honeywell Inc, C. 502.
4. Romanchenko, M. A. Mazorenko, D. I., Slesarenko, A. P., Soroka, O. S. (2006). Energozberigajuchi elektrotehnologiï zabezpechennja standartiv teplovogo rezhimu virobnichih sporud APK z elektroobigrivnimi pidlogami. Elektrifik. ta avtomatiz. sil's'kogo gospodarstva, №2, 82 - 92.
5. Tabunshhikov Ju. A. (2004). Jenergojeffektivnye zdanija: mirovoj i oteches-tvennyj opyt. Jenergija, №10, 20-28, № 11, 26-29;
6. Popescu, D. (2008) A new solution for automatic control of heating systems in buildings based on measuring heat transfer through outer surfaces. ACMOS'08 Proc. of the 10th WSEAS Int. Conf. on Automatic Control, Modelling & Simulation, 206 - 208.
7. Rozins'kij, D. J. (2002). Elektrichna kabel'na sistema opalennja v teplo-akumuljacijnomu rezhimi (EKSO-TA) zhitlovih sil's'kogospodars'kih budinkiv. Budivnictvo Ukraïni, №5, 32 - 35.
8. Dryden, I .G. C. (1982). The Efficient Use of Energy. 2nd Ed., Butterworth Scientific, Oxford.
9. Davies, E. J. (1990). Conduction and Induction Heating. IEE Power Engineering Series II, Peter Peregrinus Ltd., London.
10. Saving Energy with Electric Resistance Heating (1997). DOE/GO-10097-381, FS 230, October.
11. Domestic Heating Compliance Guide (2008). Domestic Heating Compliance Guide 2-nd edition, 72.
12. Building automation – impact on energy efficiency. Application per EN 15232:2012 eu.bac product certification (2012). Siemens Switzerland Ltd, 132.