ABSTRACT AND REFERENCES

INFORMATION AND CONTROLLING SYSTEM

**DOI:** 10.15587/1729-4061.2019.166349

**A MULTICRITERIAL ANALYSIS OF THE EFFICIENCY OF CONSERVATIVE INFORMATION SECURITY SYSTEMS (p. 6–13)**

**Valeriy Dudykevych**
Lviv Polytechnic National University, Lviv, Ukraine
**ORCID:** http://orcid.org/0000-0001-8827-9920

**Ivan Prokopyshyn**
Ivan Franko National University of Lviv, Lviv, Ukraine
**ORCID:** http://orcid.org/0000-0003-2652-1245

**Vasyl Chekurin**
Pidstryhach Institute for Applied Problems of Mechanics and Mathematics of the National Academy of Sciences of Ukraine, Lviv, Ukraine
Kujawy and Pomorze University in Bydgoszcz, Bydgoszcz, Poland
**ORCID:** http://orcid.org/0000-0003-4973-3670

**Ivan Opirskyy**
Lviv Polytechnic National University, Lviv, Ukraine
**ORCID:** http://orcid.org/0000-0002-8461-8996

**Yuriy Lakh**
Lviv Polytechnic National University, Lviv, Ukraine
**ORCID:** http://orcid.org/0000-0003-4153-8125

**Taras Kret**
Lviv Polytechnic National University, Lviv, Ukraine
**ORCID:** http://orcid.org/0000-0002-6333-3190

**Yevheniia Ivanchenko**
National Aviation University, Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0003-3017-5752

**Ihor Ivanchenko**
National Aviation University, Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0003-3415-9039

The paper addresses the task on a multicriterial analysis of the effectiveness of conservative information security systems whose structure and components do not change over a certain period of time. The principal scheme of such systems includes a protected object, vulnerabilities – channels for attacks, threats, and protection tools.

Based on the assumption about the independence of attacks and protection tools, we have developed a discrete probabilistic model of damage to a protected object. For a random variable of the amount of damage over a fixed period of time, we have derived a representation in the form of a sum of binomially-distributed random variables, dependent on the parameters for attacks and protection. We have described in a similar manner the random variables for economic losses, recovery time, as well as recovery costs, for which mathematical expectations and variances have been obtained in the analytical form. To ensure the high statistical confidence, it has been proposed to determine the risk indicators using a Cantelli's inequality. On this basis, we have defined performance indicators for a protection system, which characterize the probability of protected object's safety, residual losses, conditionally saved costs, survivability, and the cost of recovery.

By using a Pareto optimality theory, we have devised a procedure for multi-criteria analysis and rational design of conservative systems of information protection. Verification has been carried out for the audio information protection systems. A Pareto frontier has been investigated according to the criteria of economic benefit and investment costs for 66 variants of protection. We have examined the influence of protection level on the Cantelli's measure for conditional savings, as well as the contribution of various types of protection devices to it.

The research results have confirmed the saturation law by Gordon-Loeb for the case when over-protection does not improve the effectiveness of protection systems.

**Keywords:** information security systems, risk, efficiency, multicriterial analysis, Gordon-Loeb model.

**References**

1. Allianz Risk Barometer: Top Business Risks for 2018. Available at: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2018.pdf
2. Regional Risks for Doing Business 2018: Insight Report (2018). Geneva, 40. Available at: http://www3.weforum.org/docs/WEF_Regional_Risks_Doing_Business_report_2018.pdf
3. Brotby, W. K. (2009). Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement. Taylor & Francis, 200. doi: https://doi.org/10.1201/9781420052862
4. Sahinoglu, M. (2016). Cyber-Risk Informatics: engineering evaluation with data science. Wiley & Sons, 560. doi: https://doi.org/10.1002/9781119087540
5. Korchenko, O. H., Kazmirchuk, S. V., Akhmetov, B. B. (2017). Prykladni systemy otsiniuvannia ryzykiv informatsiynoi bezpeky. Kyiv, 435.
6. Yudin, A., Buchyk, S. (2016). Technology of construction and defence of the Ukrainian segment of the identifiers' tree of state informative resources on the basis of risk management. Zakhyst informatsiyi, 18 (2), 107–114. Available at: http://nbuv.gov.ua/UJRN/Zi_2016_18_2_5
7. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F. (2016). Decision support approaches for cyber security investment. Decision Support Systems, 86, 13–23. doi: https://doi.org/10.1016/j.dss.2016.02.012
8. Hu, Z., Khokhlachova, Y., Sydorenk, V., Opirskyy, I. (2017). Method for Optimization of Information Security Systems Behavior under Conditions of Influences. International Journal of Intelligent Systems and Applications, 9 (12), 46–58. doi: https://doi.org/10.5815/ijisa.2017.12.05
9. Gordon, L. A., Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5 (4), 438–457. doi: https://doi.org/10.1145/581271.581274
10. Gordon, L. A., Loeb, M. P., Zhou, L. (2016). Investing in Cybersecurity: Insights from the Gordon-Loeb Model. Journal of Information Security, 07 (02), 49–59. doi: https://doi.org/10.4236/jis.2016.72004
11. Artzner, P., Delbaen, F., Eber, J.-M., Heath, D. (1999). Coherent Measures of Risk. Mathematical Finance, 9 (3), 203–228. doi: https://doi.org/10.1111/1467-9965.00068

12. McNeil, A. J., Frey, R., Embrechts, P. (2005). Quantitative Risk Management: Concepts, Techniques and Tool. Princeton and Oxford, 538.
13. Wang, J., Chaudhury, A., Rao, H. R. (2008). Research Note – A Value-at-Risk Approach to Information Security Investment. Information Systems Research, 19 (1), 106–120. doi: https://doi.org/10.1287/isre.1070.0143
14. Raugas, M., Ulrich, J., Faux, R., Finkelstein, S., Cabot, C. (2013). CyberV@R. A Cyber Security Model for Value at Risk. Technical report. Baltimore MD, 45. Available at: https://www.cyberpointllc.com/docs/CyberVaR.pdf
15. Dudykevych, V. B., Lakh, Yu. V., Prokopyshyn, I. A. (2011). Otsinka vartosti ryzyku dlia system zakhystu informatsiyi. Informatsiyna bezpeka, 1 (5), 44–49.
16. Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. Decision Support Systems, 55 (1), 156–164. doi: https://doi.org/10.1016/j.dss.2013.01.001
17. Ross, S. M. (2002). Probability models for computer science. Elsevier Science, 288.
18. Dudykevych, V. B., Ivaniuk, V. M., Prokopyshyn, I. A. (2014). Efektyvnist investytsiy u systemy zakhystu prymishchen vid vytoku movnoi informatsiyi. Kompiuterni tekhnolohiyi drukarstva, 32, 20–28. Available at: http://nbuv.gov.ua/UJRN/Ktd_2014_32_4
19. Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., Linkov, I. (2017). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. Risk Analysis. doi: https://doi.org/10.1111/risa.12891
20. Motzek, A., Gonzalez-Granadillo, G., Debar, H., Garcia-Alfaro, J., Möller, R. (2017). Selection of Pareto-efficient response plans based on financial and operational assessments. EURASIP Journal on Information Security, 2017 (1). doi: https://doi.org/10.1186/s13635-017-0063-6
21. Dudykevych, V. B., Prokopyshyn, I. A., Chekurin, V. F. (2012). Problems of efficiency estimation of security systems. Visnyk NU «Lvivska politekhnika». Avtomatyka, vymiriuvannia ta keruvannia, 741, 118–122. Available at: http://science.lpnu.ua/uk/node/3718
22. Ehrgott, M. (2005). Multicriteria Optimization. Berlin Heidelberg, 323. doi: https://doi.org/10.1007/3-540-27659-9
23. Lakhno, V., Kozlovskii, V., Boiko, Y., Mishchenko, A., Opirskyy, I. (2017). Management of information protection based on the integrated implementation of decision support systems. Eastern-European Journal of Enterprise Technologies, 5 (9 (89)), 36–42. doi: https://doi.org/10.15587/1729-4061.2017.111081

**DOI:** 10.15587/1729-4061.2019.166504

**INTERLABORATORY COMPARISONS OF THE CALIBRATION RESULTS OF SIGNAL GENERATOR (p. 14–20)**

**Oleh Velychko**
State Enterprise «All-Ukrainian State Scientific and Production Centre for Standardization, Metrology, Certification and Protection of Consumer», (SE «Ukrmetrteststandard»), Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0002-6564-4144

**Sergii Shevkun**
State Enterprise «All-Ukrainian State Scientific and Production Centre for Standardization, Metrology, Certification and Protection of Consumer», (SE «Ukrmetrteststandard»), Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0003-1923-6227

**Oleh Mescheriak**
State Enterprise «All-Ukrainian State Scientific and Production Centre for Standardization, Metrology, Certification and Protection of Consumer», (SE «Ukrmetrteststandard»), Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0003-2844-7018

**Tetyana Gordiyenko**
Odessa State Academy of Technical Regulation and Quality, Odessa, Ukraine
**ORCID:** http://orcid.org/0000-0003-0324-9672

**Sergii Kursin**
State Enterprise «All-Ukrainian State Scientific and Production Centre for Standardization, Metrology, Certification and Protection of Consumer», (SE «Ukrmetrteststandard»), Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0003-2147-6211

The data of interlaboratory comparisons of calibration results of signal generators at three calibration points are presented. The choice of methodology for processing the results of interlaboratory comparisons is made taking into account the long-term drift of the comparison sample. The modernization and research of the comparison sample for interlaboratory comparisons of calibration results of signal generators are carried out. The assigned values for the three calibration points and their extended uncertainties are determined. Expressions are obtained for the approximation of the long-term drift of the comparison sample and uncertainty budgets for all assigned values of the comparison sample at the frequencies of 130 MHz, 168 MHz and 223 MHz are compiled.

The interlaboratory deviations of the results obtained by laboratories are determined and the consistency of the data obtained using the $E_n$ and z indicators is estimated. This characterizes the reliability and accuracy of laboratory measurement results, and is also important for confirming technical competence. The presented results of interlaboratory comparisons of the signal generator calibration results show that all participating laboratories meet the requirements by the $E_n$ indicator. At the same time, two out of ten laboratories require certain substantial corrective measures, as they do not meet the requirements by the z indicator.

It is established that the $E_n$ indicator is not always self-sufficient. It largely characterizes only the reliability of laboratory measurement results. For this purpose, the z indicator is more informative, which provides more information on the accuracy of laboratory measurement, that is, the proximity of measurement results to the true value.

**Keywords:** interlaboratory comparison, calibration laboratory, measurement uncertainty, signal generator, comparison sample.

**References**

1. International vocabulary of metrology. Basic and general concepts and associated terms (VIM) (2012). JCGM. Available at: https://www.bipm.org/utils/common/documents/jcgm/JCGM_200_2012.pdf
2. ISO/IEC Guide 98-3:2008. Uncertainty of measurement. Part 3. Guide to the expression of uncertainty in measurement (GUM:1995) (2008). ISO/IEC, 130.
3. ILAC Policy on the Traceability of Measurement Results (2013). ILAC. Available at: http://www.enao-eth.org/publication_documents/ILAC_P10_01_2013%20ILAC%20

Policy%20on%20Traceability%20of%20Measurement%20Results.pdf
4. DSTU ISO/IEC 17025:2006. General requirements for the competence of testing and calibration laboratories (ISO/IEC 17025:2005, IDT) (2007). Kyiv: Derzhspozhyvstandart Ukrainy, 32.
5. DSTU EN ISO/IEC 17043:2014. Otsinka vidpovidnosti. Zahalni vymohy do perevirky kvalifikatsiyi laboratoriy (EN ISO/IEC 17043:2010, IDT) (2014). Kyiv: Minekonomrozvytku Ukrainy, 21.
6. Velychko, O., Gordiyenko, T. (2018). Linking Results of International Comparisons of the National Standard and the National Inter-Laboratory Comparisons. Journal of Physics: Conference Series, 1065, 072004. doi: https://doi.org/10.1088/1742-6596/1065/7/072004
7. Velychko, O., Shevkun, S., Gordiyenko, T., Mescheriak, O. (2018). Interlaboratory comparisons of the calibration results of time meters. Eastern-European Journal of Enterprise Technologies, 1 (9 (91)), 4–11. doi: https://doi.org/10.15587/1729-4061.2018.121089
8. Velychko, O., Gordiyenko, T. (2010). The implementation of general international guides and standards on regional level in the field of metrology. Journal of Physics: Conference Series, 238, 012044. doi: https://doi.org/10.1088/1742-6596/238/1/012044
9. Velychko, O., Gordiyenko, T. (2015). The estimation of the measurement results with using statistical methods. Journal of Physics: Conference Series, 588, 012017. doi: https://doi.org/10.1088/1742-6596/588/1/012017
10. Efremova, N. Yu., Chunovkina, A. G. (2007). Opyt ocenivaniya dannyh mezhlaboratornyh slicheniy kalibrovochnyh i poverochnyh laboratoriy. Izmeritel'naya tekhnika, 6, 15–21.
11. Claudio, J., Costa, M. (2012). Brazilian energy interlaboratory program applicative. XX IMEKO World Congress «Metrology for Green Growth». Busan, 6.
12. Sandu, I., Dragomir, L., Pantelimon, B. (2007). Interlaboratory comparison. 15th IMEKO TC 4 Symposium on Novelties in Electrical Measurements and Instrumentations. Iasi, 4.
13. Sousa, J. J. L., Leitão, L. T. S., Costa, M. M., Faria, M. C. (2012). Considerations on the influence of travelling standards instability in an interlaboratory comparison program. XX IMEKO World Congress «Metrology for Green Growth». Busan, 4.
14. Poenaru, M. M., Iacobescu, F., Anghel, A.-C., Sălceanu, A., Anghel, M.-A. (2016). Active power quality assessment through interlaboratories comparison. 21th IMEKO TC4 International Symposium «Understanding the World through Electrical and Electronic Measurement». Budapest, 224–228.
15. Poenaru, M. M., Iacobescu, F., Anghel, M.-A. (2017). Length calibration Quality assessment through Interlaboratories Comparison. 22th IMEKO TC 4 Symposium «Supporting World development through electrical and electronic measurements». Iasi, 20–26.
16. Dierikx, E., Nestor, A., Melcher, J., Kölling, A., Callegaro, L. (2012). Final report on the supplementary comparison EURAMET.EM-S26: inductance measurements of 100 mH at 1 kHz (EURAMET project 816). Metrologia, 49 (1A), 01002–01002. doi: https://doi.org/10.1088/0026-1394/49/1a/01002
17. Çayci, H. (2011). Final report on key comparison EURAMET.EM-K5.1 (EURAMET Project No. 687): Comparison of 50/60 Hz power. Metrologia, 48 (1A), 01009–01009. doi: https://doi.org/10.1088/0026-1394/48/1a/01009
18. Johnson, L., Chua, W., Corney, A., Hsu, J., Sardjono, H., Lee, R. D. et. al. (2008). Final report on the APMP comparison of capacitance at 100 pF (APMP supplementary comparison APMP.EM-S7). Metrologia, 45 (1A), 01003–01003. doi: https://doi.org/10.1088/0026-1394/45/1a/01003
19. Oldham, N., Nelson, T., Zhang, N. F., Liu, H. (2003). CCEM-K5 Comparison of 50/60 Hz power. Metrologia, 40 (1A), 01003–01003. doi: https://doi.org/10.1088/0026-1394/40/1a/01003
20. DSTU ISO 13528:2014. Statystychni metody, shcho zastosovuiutsia pry perevirtsi kvalifikatsiyi laboratoriyi shliakhom mizhlaboratornykh porivnian (ISO 13528:2005, IDT) (2014). Kyiv: Minekonomrozvytku Ukrainy, 29.

**DOI:** 10.15587/1729-4061.2019.166994

**DEVELOPMENT OF A COMPLEX MATHEMATICAL MODEL OF THE STATE OF A CHANNEL OF MULTI-ANTENNA RADIO COMMUNICATION SYSTEMS (p. 21–30)**

**Svitlana Kalantaievska**
Military Institute of Telecommunications and Informatization named after Heroes of Kruty, Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0001-6426-2235

**Oleksii Kuvshynov**
Ivan Chernyakhovsky National Defense University of Ukraine, Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0003-2183-7224

**Andrii Shyshatskyi**
Central Scientific Research Institute of Armament and Military Equipment of the Ukrainian Armed Forces, Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0001-6731-6390

**Olha Salnikova**
Ivan Chernyakhovsky National Defense University of Ukraine, Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0002-7190-6091

**Yurii Punda**
Ivan Chernyakhovsky National Defense University of Ukraine, Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0002-1431-2318

**Pavlo Zhuk**
Ivan Chernyakhovsky National Defense University of Ukraine, Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0002-9628-8074

**Olesia Zhuk**
Military Institute of Telecommunications and Informatization named after Heroes of Kruty, Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0002-8974-0309

**Hryhorii Drobakha**
National Academy of the National Guard of Ukraine, Kharkiv, Ukraine
**ORCID:** http://orcid.org/0000-0001-7644-8838

**Lyubov Shabanova-Kushnarenko**
National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine
**ORCID:** http://orcid.org/0000-0002-2080-7173

**Sergii Petruk**
Central Scientific Research Institute of Armament and Military Equipment of the Ukrainian Armed Forces, Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0002-0709-0032

The complex mathematical model of the state of the channel of multi-antenna radio communication systems is developed. The model takes into account: the effect of intentional noise and signal fading, the number of receiving antennas, Doppler effect, correlation coefficient, speed and direction of the receiver and the transmitter, intersymbol interference, phase jitter and inclination of the constellation matrix. Simulation of the state of the channel of multi-antenna radio communication systems is carried out for each individual antenna channel, after which a generalized estimate is formed at the output. The development of the proposed integrated mathematical model is due to the need to improve the accuracy of the description of the channel state of multi-antenna radio communication systems with an acceptable computational complexity. The proposed model allows to improve the accuracy of the description of the state of the channel of multi-antenna radio communication systems by taking into account additional destabilizing factors, thereby increasing the accuracy of the channel state assessment. I would like to note that at the same time there is an increase in the computational complexity at the level of 5–7 % due to an increase in the number of evaluated indicators. The mentioned complex mathematical model should be used in radio stations with a programmable architecture to increase their noise immunity by increasing the accuracy of the evaluation of the characteristics of the receiving and transmitting path relative to the state of the channel. The research of the correlation between antennas of multi-antenna radio communication systems was conducted. The results show that in the presence of a line of sight between the receiver and the transmitter, the signal correlation is high and therefore a small increase is expected from the use of several antennas, and in the absence of line of sight conditions, the signal correlation is low.

**Keywords:** radio communication devices, Jakes model, Doppler spectrum, computational complexity, constellation matrix, noise immunity.

**References**

1. Slyusar, V. (2005). Cistemy MIMO: principy postroeniya i obrabotka signalov. Elektronika: Nauka, Tekhnologiya, Biznes, 8, 52–58.
2. Kuvshynov, O. V. (2009). Adaptyvne upravlinnia zasobamy zavadozakhystu viyskovykh system radiozviazku. Zbirnyk naukovykh prats VIKNU, 17, 125–130.
3. Jia, R., Li, Y., Cheng, X., Ai, B. (2018). 3D geometry-based UAV-MIMO channel modeling and simulation. China Communications, 15 (12), 64–74.
4. Ma, Y., Yang, L., Zheng, X. (2018). A geometry-based non-stationary MIMO channel model for vehicular communications. China Communications, 15 (7), 30–38. doi: https://doi.org/10.1109/cc.2018.8424580
5. Zhu, Q., Jiang, K., Chen, X., Zhong, W., Yang, Y. (2018). A novel 3D non-stationary UAV-MIMO channel model and its statistical properties. China Communications, 15 (12), 147–158.
6. Jiang, H., Zhang, Z., Wu, L., Dang, J. (2018). Three-Dimensional Geometry-Based UAV-MIMO Channel Modeling for A2G Communication Environments. IEEE Communications Letters, 22 (7), 1438–1441. doi: https://doi.org/10.1109/lcomm.2018.2828110
7. Kamga, G. N., Xia, M., Aissa, S. (2017). Spectral-Efficiency Analysis of Regular- and Large-Scale (Massive) MIMO With a Comprehensive Channel Model. IEEE Transactions on Vehicular Technology, 66 (6), 4984–4996. doi: https://doi.org/10.1109/tvt.2016.2620489
8. Nadeem, Q.-U.-A., Kammoun, A., Debbah, M., Alouini, M.-S. (2015). 3D Massive MIMO Systems: Modeling and Performance Analysis. IEEE Transactions on Wireless Communications, 14 (12), 6926–6939. doi: https://doi.org/10.1109/twc.2015.2462828
9. Vaezi, A., Abdipour, A., Mohammadi, A., Ghannouchi, F. M. (2017). On the Modeling and Compensation of Backward Crosstalk in MIMO Transmitters. IEEE Microwave and Wireless Components Letters, 27 (9), 842–844. doi: https://doi.org/10.1109/lmwc.2017.2734751
10. Yang, M., Zhang, S., Shao, X., Guo, Q., Tang, W. (2017). Statistical modeling of the high altitude platform dual-polarized MIMO propagation channel. China Communications, 14 (3), 43–54. doi: https://doi.org/10.1109/cc.2017.7897321
11. Wu, H., Gao, X., You, X. (2016). Robust Equalizer for Multicell Massive MIMO Uplink With Channel Model Uncertainty. IEEE Transactions on Vehicular Technology, 65 (5), 3231–3242. doi: https://doi.org/10.1109/tvt.2015.2442996
12. Chatterjee, S., Chatterjee, A., Das, S. S. (2018). Analytical Performance Evaluation of Full-Dimensional MIMO Systems Using Realistic Spatial Correlation Models. IEEE Transactions on Vehicular Technology, 67 (7), 5597–5612. doi: https://doi.org/10.1109/tvt.2018.2801825
13. Li, J., Ai, B., He, R., Yang, M., Zhong, Z. (2019). On Modeling of Dense Multipath Component for Indoor Massive MIMO Channels. IEEE Antennas and Wireless Propagation Letters, 18 (3), 526–530. doi: https://doi.org/10.1109/lawp.2019.2896088
14. Chen, J., Yin, X., Cai, X., Wang, S. (2017). Measurement-Based Massive MIMO Channel Modeling for Outdoor LoS and NLoS Environments. IEEE Access, 5, 2126–2140. doi: https://doi.org/10.1109/access.2017.2652983
15. Tan, W., Jin, S., Yuan, J. (2017). Spectral and energy efficiency of downlink MU-MIMO systems with MRT. China Communications, 14 (5), 105–111. doi: https://doi.org/10.1109/cc.2017.7942318
16. Song, J., Choi, J., Kim, T., Love, D. J. (2018). Advanced Quantizer Designs for FDD-Based FD-MIMO Systems Using Uniform Planar Arrays. IEEE Transactions on Signal Processing, 66 (14), 3891–3905. doi: https://doi.org/10.1109/tsp.2018.2839588
17. He, H., Wen, C.-K., Jin, S., Li, G. Y. (2018). Deep Learning-Based Channel Estimation for Beamspace mmWave Massive MIMO Systems. IEEE Wireless Communications Letters, 7 (5), 852–855. doi: https://doi.org/10.1109/lwc.2018.2832128
18. Ampoma, A. E., Wen, G., Huang, Y., Gyasi, K. O., Tebe, P. I., Ntiamoah-Sarpong, K. (2018). Spatial Correlation Models of Large-Scale Antenna Topologies Using Maximum Power of Offset Distribution and its Application. IEEE Access, 6, 36295–36304. doi: https://doi.org/10.1109/access.2018.2846260
19. Kalantaijevska, S. (2018). Analysis of the effect of destabilizing factors on multipleaning of military radio communication systems. Zbirnyk naukovykh prats VITI, 2, 49–56.
20. Zaitsev, S. V. (2012). Doslidzhennia vplyvu navmysnykh zavad na propusknu spromozhnist zasobiv radiozviazku z tekhnolohieiu MIMO-OFDM. Matematychni mashyny i systemy, 1, 139–153.
21. Home of the Coded Modulation Library. Available at: http://www.iterativesolutions.com/
22. Zhyvotovskyi, R., Shyshatskyi, A., Petruk, S. (2017). Structural-semantic model of communication channel. 2017 4th International Scientific-Practical Conference Problems of

Infocommunications. Science and Technology (PIC S&T). doi: https://doi.org/10.1109/infocommst.2017.8246454
23. Goldsmith, A., Jafar, S. A., Jindal, N., Vishwanath, S. (2003). Capacity limits of MIMO channels. IEEE Journal on Selected Areas in Communications, 21 (5), 684–702. doi: https://doi.org/10.1109/jsac.2003.810294
24. Kalantaievska, S., Pievtsov, H., Kuvshynov, O., Shyshatskyi, A., Yarosh, S., Gatsenko, S. et. al. (2018). Method of integral estimation of channel state in the multiantenna radio communication systems. Eastern-European Journal of Enterprise Technologies, 5 (9 (95)), 60–76. doi: https://doi.org/10.15587/1729-4061.2018.144085
25. Petruk, S., Zhyvotovskyi, R., Shyshatskyi, A. (2018). Mathematical Model of MIMO. 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). doi: https://doi.org/10.1109/infocommst.2018.8632163

**DOI:** 10.15587/1729-4061.2019.168525

**CONSTRUCTION OF A GENERALIZED PROBABILISTIC-PHYSICAL MODEL OF RELIABILITY OF A TWO-LEVEL ACTIVE PHASED ANTENNA ARRAY (p. 31–40)**

**Valery Kostanovskyi**
State Enterprise Research Institute «Kvant», Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0002-3766-4455

**Igor Machalin**
National Aviation University, Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0003-1684-4980

**Oksana Kozachuk**
State Enterprise Research Institute «Kvant», Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0003-0905-1093

**Irina Terentyeva**
National Aviation University, Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0002-0391-5041

A generalized probabilistic-physical model of reliability of a two-level active phased antenna array (APAA) of a multifunctional radar station was presented.

When constructing the APAA physical model, definitions of failures of the radiating channel and the antenna array as a whole were formulated. Key parameters of the APAA were chosen: radiation power, gain in transmission and the top level of the near side lobes. This has made it possible to formulate generalized criteria of failure of the APAA operating in the modes of transmission and reception as well as determine the permissible number of failures of the radiating channels and receiving modules. The physical model of the APAA reliability was formalized by a system of equations describing deviation of key parameters of the antenna array beyond the permissible limits. At the same time, boundary (permissible) values of the number of failed radiating channels and receiving modules were found that provide critical (minimum permissible) values of key parameters of the antenna array.

To construct a probabilistic model of the APAA reliability, the antenna array was defined as an isotropic hierarchical system and a formula was derived for determining the average number of operable radiating channels in the multi-level APAA structure. A block-diagram of reliability of receiving and transmitting sub-arrays, receiving and transmitting APAA has been built and formalized. Definition of failures of the receiving and transmitting sub-arrays, receiving and transmitting APAA was given. This has allowed us to derive analytical expressions for determining mean time to failure, probability of failure-free operation, density of time to failure and failure rates for sub-arrays and the APAA. Exponential distribution (for sudden failures), diffusional non-monotonic distribution (for gradual failures) and composition of exponential and diffusional non-monotonic distributions (at a joint manifestation of sudden and gradual failures) were used as models of failure of SHF elements, transistors, radiating channels and receiving modules. An illustrative example of calculation of the average time to failure of a two-level APAA of a multifunctional RS including 6400 radiating channels was presented.

**Keywords:** mean time to failure, phased antenna array, failure criteria, radiating channels.

**References**

1. Brookner, E. (2000). Phased arrays for the new millennium. Proceedings 2000 IEEE International Conference on Phased Array Systems and Technology (Cat. No.00TH8510). doi: https://doi.org/10.1109/past.2000.858889
2. Delaney, W. (2016). From vision to reality 50+ years of phased array development. 2016 IEEE International Symposium on Phased Array Systems and Technology (PAST). doi: https://doi.org/10.1109/array.2016.7832536
3. Voskresenskiy, D. I. (Ed.) (2012). Ustroystva SVCH i antenny. Proektirovanie fazirovannyh antennyh reshetok. Moscow: izd. Radiotekhnika, God izd., 744.
4. GOST 27.301-95. Nadezhnost' v tekhnike. Raschet nadezhnosti. Osnovnye polozheniya (1995). Moscow: Izd-vo standartov, 15.
5. GOST 27.003-2016. Nadezhnost' v tekhnike. Sostav i obschie pravila zadaniya trebovaniy po nadezhnosti (2016). Moscow: Izd-vo «Standartinform», 18.
6. Kartsan, I. N., Kiseleva, E. A., Logacheva, A. I., Kartsan, T. I. (2017). Dependence of the characteristics of the active phased array antenna on the time. Science Almanac, 7-1 (33), 182–192.
7. Agrawal, A. K., Holzman, E. L. (1999). Active phased array design for high reliability. IEEE Transactions on Aerospace and Electronic Systems, 35 (4), 1204–1211. doi: https://doi.org/10.1109/7.805438
8. Agrawal, A. K., Holzman, E. L. (1999). Beamformer architectures for active phased-array radar antennas. IEEE Transactions on Antennas and Propagation, 47 (3), 432–442. doi: https://doi.org/10.1109/8.768777
9. Agrawal, A. K., Kopp, B. A., Luesse, M. H., O'Haver, K. W. (2001). Active Phased Array Antenna Development for Modern Shipboard Radar Systems. Johns Hopkins APL Technical Digest, 22 (4), 600–613.
10. Antoshina, V. M., Yakimov, V. L. (2018). Description of multifunctional radar stations constructive failure statistics elem ents by experim ental data. Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki, 12, 396–404.
11. Antoshina, V. M., Babkin, Yu. V., Trunov, S. Yu., Hodataev, N. A. (2016). Metody operativnoy proverki rabotosposobnosti sistem RLS dal'nego deystviya. Ist. «Mintsevskie chteniya» trudy Tret'ey Vseross. NTK molodyh konstrukt. i inzh., posvyaschennoy 70 – letiyu Radiotekhn. Inst. imeni akad. A. L. Mintsa i 70 – letiyu FizTekha. Moscow, 100–107.
12. Kostanovskyi, V. V. A Mathematical Model for Calculating the Reliability of Nonreducible Phased Antenna

Arrays. Measurement Techniques, 57 (1), 87–90. doi: https://doi.org/10.1007/s11018-014-0412-5
13. Belyaev, Yu. K., Bogatyrev, V. A., Bolotin, V. V. et. al.; Ushakov, I. A. (Ed.) (1985). Cpravochnik. Nadezhnost' tekhnicheskih sistem. Moscow: Izd. «Radio i svyaz'», 606.
14. Kostanovskyi, V. V., Kozachuk, O. D. (2015). Veroyatnostniy analiz bezotkaznosti i dolgovechnosti apertur fazirovannyh antennyh reshetok v protsesse proektirovaniya. Matematychni mashyny i systemy, 3, 201–213.
15. Kostanovskyi, V. V. (2014). Matematychni modeli nadiynosti typovykh apertur fazovanykh antennykh reshitok, yaki vrakhovuiut raptovi ta postupovi vidmovy moduliv nadvysokykh chastot. Matematychni mashyny i systemy, 2, 142–150.
16. GOST 23282-91. Reshetki antennye. Terminy i opredeleniya (1991). Moscow, 7.
17. GOST 27.002-2015. Nadezhnost' v tekhnike. Terminy i opredeleniya. Dependability in technics. Terms and definitions (2015). Moscow, 28.
18. GOST 27.310-95. Nadezhnost' v tekhnike. Analiz vidov, posledstviy i kritichnosti otkazov. Osnovnye polozheniya (1995). Moscow, 20.
19. Azarskov, V. N., Strel'nikov, V. P. (2004). Nadezhnost' sistem upravleniya i avtomatiki. Kyiv: NAU, 164.
20. Kostanovskyi, V., Kozachyk, O. (2018). The method of identifying the parameters of the universal model of failures approximating the generalized curve of the failure rate of electronic products. Science-based technologies, 4 (40), 465–472. doi: https://doi.org/10.18372/2310-5461.40.13273
21. Kaganov, V. L., Kapitonov, V. A. (1984). Obobschennaya model' nadezhnosti i otrabotochnye ispytaniya. Vibratsionnaya prochnost' i nadezhnost' dvigateley i sistem letatel'nyh apparatov, 10, 83–90.
22. Spravochnik. Nadezhnost' elektroradioizdeliy – 2002 (2002). Sankt-Peterburg, 574.

**DOI:** 10.15587/1729-4061.2019.166887

**APPLICATION OF KOHONEN NEURAL NETWORKS TO SEARCH FOR REGIONS OF INTEREST IN THE DETECTION AND RECOGNITION OF OBJECTS (p. 41–48)**

**Victor Skuratov**
Joint-stock company All-Russian Scientific Research Institute of Radio Engineering, Moscow, Russian Federation
**ORCID:** http://orcid.org/0000-0003-1526-1505

**Konstantin Kuzmin**
University of Russian Innovation Education, Moscow, Russian Federation
**ORCID:** http://orcid.org/0000-0003-3823-7268

**Igor Nelin**
Moscow Aviation Institute, Moscow, Russian Federation
**ORCID:** http://orcid.org/0000-0003-0469-6650

**Mikhail Sedankin**
Main Research and Testing Robotics Centre of the Ministry of Defence of the Russian Federation, Moscow, Russian Federation
State Research Center – Burnasyan Federal Medical Biophysical Center of Federal Medical Biological Agency, Moscow, Russian Federation
**ORCID:** http://orcid.org/0000-0001-9875-6313

One of the most effective ways to improve accuracy and speed of recognition algorithms is to preliminary distinguish the regions of interest in the analyzed images. We studied a possibility of application of self-organizing maps and a Kohonen neural network for detection of regions of interest at a radar or satellite image of underlying surface. There is a high probability of finding an object of interest for further analysis in the found regions of interest. The definition of region of interest is necessary most of all to automate and speed up the process of search and recognition of objects of interest. The relevance is due to the increasing number of satellites. The study presents the process of modeling, analysis and comparison of the results of application of these methods for determination of regions of interest in recognition of images of aircraft against the background of underlying surface. It also describes the process of preliminary processing of input data. The study presents a general approach to construction and training of the Kohonen self-organizing map and neural network. Application of Kohonen maps and neural network makes it possible to decrease an amount of data analyzed by 15–100 times. It speeds up the process of detection and recognition of an object of interest. Application of the above algorithm reduces significantly the required number of training images for a convolutional network, which performs the final recognition. The reduction of a training sample occurs because the size of parts of an input image supplied to the convolutional network is bounded with the scale of an image and it is equal to the size of the largest detected object. Kohonen neural network showed itself more efficient in relation to this task, since it places cluster centers on the underlying surface rarely due to independence of weight of neurons on neighboring centers. These technical solutions could be used in the analysis of visual data from satellites, aircraft, and unmanned cars, in medicine, robotics, etc.

**Keywords:** image recognition, self-organizing maps, Kohonen neural network, radar and satellite images, region of interest, ROI, test operations procedure, robotics.

**References**

1. Simard, P. Y., Steinkraus, D., Platt, J. C. (2003). Best practices for convolutional neural networks applied to visual document analysis. Proceedings of the Seventh International Conference on Document Analysis and Recognition. Available at: http://cognitivemedium.com/assets/rmnist/Simard.pdf
2. Novikova, N. M., Dudenkov, V. M. (2015). Modelirovanie neyronnoy seti dlya raspoznavaniya izobrazheniy na osnove gibridnoy seti i samoorganizuyuschihsya kart Kohonena. Aspirant, 2, 31–34.
3. Agayan, K. Yu., Hanzhin, V. G. (2018). Neyronnaya set' s arhitekturoy Kohonena dlya raspoznavaniya izobrazheniy. Prochnost' neodnorodnyh struktur – PROST 2018. Sbornik trudov IX-oy Evraziyskoy nauchno-prakticheskoy konferencii, 153.
4. Gerasimova, N. I., Verhoturova, A. E. (2014). Poisk fragmenta izobrazheniya s ispol'zovaniem neyronnoy seti Kohonena. Informacionnye tekhnologii v nauke, upravlenii, social'noy sfere i medicine: sbornik nauchnyh trudov Mezhdunarodnoy konferencii s mezhdunarodnym uchastiem. Ch. 1. Tomsk, 68–70.
5. Soldatova, O. P., Chayka, P. D. (2015). Efficiency analysis of solution of classification using hybrid kohonen neural networks. Izvestiya Samarskogo nauchnogo centra Rossiyskoy akademii nauk, 17 (2), 1147–1152.

6. Narushev, I. R. (2018). Neural network on the basis of the self-organizing kochonen card as a means of detecting anomalous behavior. Ohrana, bezopasnost', svyaz', 2 (3 (3)), 194–197.
7. Kajan, S., Sekaj, I., Lajtman, M. Cluster Analysis Aplications in Matlab Using Kohonen Network. Available at: https://pdfs.semanticscholar.org/a8ba/6977dce4bdbeec3dd370eb614de2c6f56514.pdf
8. LeCun, Y., Bengio, Y. (1998). Convolutional networks for images, speech, and time series. The handbook of brain theory and neural networks, 255–258.
9. LeCun, Y., Kavukcuoglu, K., Farabet, C. (2010). Convolutional networks and applications in vision. Proceedings of 2010 IEEE International Symposium on Circuits and Systems. doi: https://doi.org/10.1109/iscas.2010.5537907
10. Girshick, R., Donahue, J., Darrell, T., Malik, J. (2014). Rich Feature Hierarchies for Accurate Object Detection and Semantic Segmentation. 2014 IEEE Conference on Computer Vision and Pattern Recognition. doi: https://doi.org/10.1109/cvpr.2014.81
11. Girshick, R., Donahue, J., Darrell, T., Malik, J. (2016). Region-Based Convolutional Networks for Accurate Object Detection and Segmentation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 38 (1), 142–158. doi: https://doi.org/10.1109/tpami.2015.2437384
12. Girshick, R. (2015). Fast R-CNN. 2015 IEEE International Conference on Computer Vision (ICCV). doi: https://doi.org/10.1109/iccv.2015.169
13. Ren, S. et. al. (2015). Faster R-CNN: Towards real-time object detection with region proposal networks. Advances in neural information processing systems, 91–99.
14. He, K., Gkioxari, G., Dollar, P., Girshick, R. (2017). Mask R-CNN. 2017 IEEE International Conference on Computer Vision (ICCV). doi: https://doi.org/10.1109/iccv.2017.322
15. Redmon, J., Divvala, S., Girshick, R., Farhadi, A. (2016). You Only Look Once: Unified, Real-Time Object Detection. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). doi: https://doi.org/10.1109/cvpr.2016.91
16. Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C.-Y., Berg, A. C. (2016). SSD: Single Shot MultiBox Detector. Computer Vision – ECCV 2016, 21–37. doi: https://doi.org/10.1007/978-3-319-46448-0_2
17. Haykin, S. (2008). Neyronnye seti: polnyy kurs. Moscow: Izdatel'skiy dom Vil'yams.
18. Kohonen, T. (2001). Self-organizing maps. Vol. 30. Springer Science & Business Media, 502. doi: https://doi.org/10.1007/978-3-642-56927-2
19. Gersho, A., Gray, R. M. (1992). Vector quantization and signal compression. Vol. 159. Springer Science & Business Media, 732. doi: https://doi.org/10.1007/978-1-4615-3626-0


**DOI:** 10.15587/1729-4061.2019.169527

**DEVELOPMENT OF A METHODOLOGY FOR BUILDING AN INFORMATION SECURITY SYSTEM IN THE CORPORATE RESEARCH AND EDUCATION SYSTEM IN THE CONTEXT OF UNIVERSITY AUTONOMY (p. 49–63)**

**Serhii Yevseiev**
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
**ORCID:** http://orcid.org/0000-0003-1647-6444

**Volodymyr Aleksiyev**
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
**ORCID:** http://orcid.org/0000-0001-6767-7524

**Svitlana Balakireva**
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
**ORCID:** http://orcid.org/0000-0003-2535-0798

**Yevhen Peleshok**
National Technical University of Ukraine «Igor Sikorsky Kiev Polytechnic Institute», Kyiv, Ukraine
**ORCID:** http://orcid.org/0000-0003-0033-1160

**Oleksandr Milov**
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
**ORCID:** http://orcid.org/0000-0001-6135-2120

**Oleksii Petrov**
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
**ORCID:** http://orcid.org/0000-0002-3062-9286

**Olena Rayevnyeva**
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
**ORCID:** http://orcid.org/0000-0003-0260-4249

**Bogdan Tomashevsky**
Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine
**ORCID:** http://orcid.org/0000-0002-1934-4773

**Ivan Tyshyk**
Lviv Polytechnic National University, Lviv, Ukraine
**ORCID:** http://orcid.org/0000-0003-1465-5342

**Olexander Shmatko**
National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine
**ORCID:** http://orcid.org/0000-0002-2426-900X

The development of computing tools and technologies of corporate networks has expanded the range of educational and information services in corporate research and education networks (CRES). CRES belong to critical cybernetic information systems (CCIS) built on the basis of open network models. In the early 80s of the 20th century, this approach did not consider the need to build a security system, which does not allow it to provide the required level of protection against modern hybrid threats. The transition to autonomy in decision-making, education and university management all over the world places requirements to ensuring the required quality of service (QoS) of CRES clients. CRES users include university administration, faculty, students and support personnel of educational services in higher education institutions. One of the main criteria for QoS is information security. However, there is no general approach to building integrated information security in CRES, which would provide the required level of security.

The methodology is based on the concept of synthesizing a synergistic model of threats to CCIS, improved models of CRES infrastructure, an intruder, assessing the current state of information security (IS) and improved method of

investment in the CRES IS. It is shown that the basis of the synergistic model is a three-level model of strategic security management, which provides a synergistic effect in the context of simultaneous threats to information security, cybersecurity and security of information. In contrast to the known, such an approach provides for the determination of qualitatively new and previously unknown emergent properties of the information security system, taking into account the means used to create it. The application of the methodology in practice through the development and implementation of new solutions to provide security services allows for the required level of information security in CRES. The proposed information security service mechanisms are built on hybrid cryptosystems based on crypto-code structures with flawed codes.

**Keywords:** corporate research and education system, security threat classifier, information security system.

**References**

1. Androshchuk, H. O. (2017). Kiberbezpeka: tendentsiyi v sviti ta Ukraini. Kiberbezpeka ta intelektualna vlasnist: problemy pravovoho zabezpechennia: materialy Mizhnarodnoi naukovo-praktychnoi konferentsiyi. Kyiv: Vyd-vo «Politekhnika», 30–36.
2. Grischuk, R. V., Danik, Yu. G.; Danik, Yu. G. (Ed.) (2016). Osnovy kiberbezopasnosti. Zihtomir: ZHNAEU, 636.
3. Yevseiev, S., Ponomarenko, V., Ponomarenko, V., Rayevnyeva, O., Rayevnyeva, O. (2017). Assessment of functional efficiency of a corporate scientific-educational network based on the comprehensive indicators of quality of service. Eastern-European Journal of Enterprise Technologies, 6 (2 (90)), 4–15. doi: https://doi.org/10.15587/1729-4061.2017.118329
4. Hryshchuk, R. V., Korchenko, O. H. (2012). Metodolohiya syntezu ta analizu dyferentsialno-ihrovykh modelei ta metodiv modeliuvannia protsesiv kibernapadu na derzhavni informatsiyni resursy. Ukrainian Information Security Research Journal, 14 (3), 115–122. doi: https://doi.org/10.18372/2410-7840.14.3418
5. Baranov, H., Zakharova, M., Hornitska, D. (2012). Methodology for the synthesis of systems security level evaluation of public information resources from social engineering attacks. Ukrainian Information Security Research Journal, 14 (3), 98–104. doi: https://doi.org/10.18372/2410-7840.14.3396
6. Korchenko, A., Luttskyy, M., Zaharova, M., Dreys, Y. (2013). Synthesis methodology and software implementation system evaluation harm to national security in protection of state secrets. Ukrainian Information Security Research Journal, 15 (1), 14–20. doi: https://doi.org/10.18372/2410-7840.15.4210
7. Rajba, S., Karpinski, M., Korchenko, O. (2014). Generalized models, construction methodology and the application of secure wireless sensor networks with random network parameters. Ukrainian Scientific Journal of Information Security, 20 (2), 120–125. doi: https://doi.org/10.18372/2225-5036.20.7296
8. Yudin, A., Buchyk, S. (2015). Methodology of defence of state informative resources. Comparative analysis of basic terms and determinations. Ukrainian Information Security Research Journal, 17 (3), 218–225. doi: https://doi.org/10.18372/2410-7840.17.9518
9. Zhurilenko, B. (2015). Construction and analysis methodology of complex technical information security with probabilistic reliability and counting of temporal breaking attempts. Ukrainian Information Security Research Journal, 17 (3), 196–204. doi: https://doi.org/10.18372/2410-7840.17.9515
10. Buchyk, S. (2016). The methodology of analysis of risks of tree that identifiers the state informative resources. Ukrainian Information Security Research Journal, 18 (1), 81–89. doi: https://doi.org/10.18372/2410-7840.18.10116
11. Korchenko, A., Shcherbyna, V., Vyshnevska, N. (2016). A methodology for building cyberattack-generated anomaly detection systems. Ukrainian Information Security Research Journal, 18 (1), 30–38. doi: https://doi.org/10.18372/2410-7840.18.10110
12. Ivanchenko, E., Kazmirchuk, S., Gololobov, A. (2012). Metodologiya sinteza sistem analiza i otsenki riskov poter' informatsionnyh resursov. Ukrainian Information Security Research Journal, 14 (2), 5–9. doi: https://doi.org/10.18372/2410-7840.14.2178
13. Shiyan, A. (2016). Methodology of complex security for the person and social groups against the negative information-psychological influence. Ukrainian Scientific Journal of Information Security, 22 (1), 94–98. doi: https://doi.org/10.18372/2225-5036.22.10460
14. Korchenko, O., Kazmirchuk, S., Ivanchenko, E. (2017). The methodology for the synthesis of adaptive risk assessment systems of security information system resources. Ukrainian Information Security Research Journal, 19 (3), 198–204. doi: https://doi.org/10.18372/2410-7840.19.11898
15. Boyarov, E. N. (2016). Klyuchevye problemy informatsionnoy bezopasnosti sfery obrazovaniya. Pedagogika vysshey shkoly, 3.1, 42–45. Available at: https://moluch.ru/th/3/archive/43/1500/
16. Dorozhkin, A. V., Yasenev, V. N., Yasenev, O. V. (2016). Metodologicheskie aspekty obespecheniya informatsionnoy bezopasnosti v VUZe. Innovatsionnye metody obucheniya v vysshey shkole, 77–83.
17. Hryshchuk, R., Yevseiev, S. Shmatko, A. (2018). Construction methodology of information security system of banking information in automated banking systems. Vienna: Premier Publishing s. r. o., 284. doi: https://doi.org/10.29013/r.hryshchuk_s.yevseiev_a.shmatko.cmissbiabs.284.2018
18. Ansari, M. T. J., Pandey, D., Alenezi, M. (2018). STORE: Security Threat Oriented Requirements Engineering Methodology. Journal of King Saud University – Computer and Information Sciences. doi: https://doi.org/10.1016/j.jksuci.2018.12.005
19. Timpson, D., Moradian, E. (2018). A Methodology to Enhance Industrial Control System Security. Procedia Computer Science, 126, 2117–2126. doi: https://doi.org/10.1016/j.procs.2018.07.240
20. Misuri, A., Khakzad, N., Reniers, G., Cozzani, V. (2018). A Bayesian network methodology for optimal security management of critical infrastructures. Reliability Engineering & System Safety. doi: https://doi.org/10.1016/j.ress.2018.03.028
21. Mukhtar, N., Mehrabi, M., Kong, Y., Anjum, A. (2018). Machine-Learning-Based Side-Channel Evaluation of Elliptic-Curve Cryptographic FPGA Processor. Applied Sciences, 9 (1), 64. doi: https://doi.org/10.3390/app9010064
22. Rehman, S., Gruhn, V. (2018). An Effective Security Requirements Engineering Framework for Cyber-Physical Systems. Technologies, 6 (3), 65. doi: https://doi.org/10.3390/technologies6030065
23. Bodei, C., Chessa, S., Galletta, L. (2019). Measuring security in IoT communications. Theoretical Computer Science, 764, 100–124. doi: https://doi.org/10.1016/j.tcs.2018.12.002

24. Hudic, A., Smith, P., Weippl, E. R. (2017). Security assurance assessment methodology for hybrid clouds. Computers & Security, 70, 723–743. doi: https://doi.org/10.1016/j.cose.2017.03.009
25. Alguliyev, R., Imamverdiyev, Y., Sukhostat, L. (2018). Cyber-physical systems and their security issues. Computers in Industry, 100, 212–223. doi: https://doi.org/10.1016/j.compind.2018.04.017
26. Rezgui, Y., Marks, A. (2008). Information security awareness in higher education: An exploratory study. Computers & Security, 27 (7-8), 241–253. doi: https://doi.org/10.1016/j.cose.2008.07.008
27. Schneider, F. B. (2013). Cybersecurity Education in Universities. IEEE Security & Privacy, 11 (4), 3–4. doi: https://doi.org/10.1109/msp.2013.84
28. Conklin, A. (2006). Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course. Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). doi: https://doi.org/10.1109/hicss.2006.110
29. Lakhno, V. A., Kasatkin, D. Y., Blozva, A. I., Gusev, B. S. (2020). Method and Model of Analysis of Possible Threats in User Authentication in Electronic Information Educational Environment of the University. Advances in Computer Science for Engineering and Education II, 600–609. doi: https://doi.org/10.1007/978-3-030-16621-2_56
30. Akhmetov, B., Lakhno, V., Akhmetov, B., Myakuhin, Y., Adranova, A., Kydyralina, L. (2019). Models and Algorithms of Vector Optimization in Selecting Security Measures for Higher Education Institution's Information Learning Environment. Intelligent Systems in Cybernetics and Automation Control Theory, 135–142. doi: https://doi.org/10.1007/978-3-030-00184-1_13
31. Kolgatin, A. G. (2014). Informatsionnaya bezopasnost' v sistemah otkrytogo obrazovaniya. Obrazovatel'nye tekhnologii i obschestvo, 417–425.
32. Anikin, V., Emaletdinova, L. Yu., Kirpichnikov, A. P. (2015). Metody otsenki i upravleniya riskami informatsionnoy bezopasnosti v korporativnyh informatsionnyh setyah. Vestnik Kazanskogo tekhnologicheskogo universiteta, 18 (6), 195–197.
33. Litvinov, V. A., Lypko, E. V., Yakovleva, A. A. Informatsionnaya bezopasnost' vysshego uchebnogo zavedeniya v ramkah sovremennoy globalizatsii. Available at: http://conference.osu.ru/assets/files/conf_reports/conf13/132.doc
34. Vahonin, S. (2014). Udalennyy dostup i utechka dannyh. Informatsionnaya bezopasnost', 5. Available at: http://www.itsec.ru/articles2/Inf_security/udalennyy-dostup-i-utechka-dannyh/
35. Zamaraeva, O. A., Titov, V. A., Kuzin, D. O. (2014). Development of policy of information security for economic higher education institution: definition of information which is subject to protection, and creation of model of the malefactor. Modern problems of science and education, 3. Available at: https://www.science-education.ru/ru/article/view?id=13106
36. Stepanova, I. V., Mohammed Omar, A. A. (2017). Use of advanced technologies for development distributed corporate communication networks. T-Comm, 11 (6), 10–15.
37. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et. al. (2018). Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. doi: https://doi.org/10.15587/1729-4061.2018.150903
38. Yevseiev, S. (2017). The use of damaged codes in crypto code systems. Systemy obrobky informatsiyi, 5 (151), 109–121. doi: https://doi.org/10.30748/soi.2017.151.15