

## DEVELOPING WI-FI NETWORK MODEL FOR INTRUSION PREVENTION (p. 4-8)

Ivan Antipov, Tetyana Vasilenko, Ivan Mikheev

The model structure, which emulates the operation of a wireless Wi-Fi network and takes into account a possibility of intrusions, disruptions and interferences using the Delphi software application, designed solely for testing the offered algorithms of its protection, based on a fuzzy logic, is proposed in the paper. The functions of existing modeling systems, their advantages and disadvantages were analyzed. It was concluded that formerly created software programs are not suitable for this task, so the problem of developing a special model, which emulates the Wi-Fi network operation, designed solely for testing the offered algorithms of its protection, is topical today.

The main modeling stages are further considered in the paper. At the first stage, the wireless network operation, implemented by means of a centralized coordination function, is considered. The operation algorithms for separate data transmit/receive sections are given.

The procedures, specified by the algorithm, are virtually carried out on different devices. For implementing all algorithms on a computer, they were divided into several non-simultaneous procedures. At the second stage of modeling, the implementation of intruders' actions is studied. Security threats of wireless networks are considered in detail. Common attacks along with the software implementation such improper activities in the model are described

**Keywords:** wireless network, Wi-Fi network model, security

### References

1. Antipov, I. E., Vasilenko, T. A., Mikheev, I. V. (2011). Primenenie nechetkoy logiki dlya povysheniya bezopasnosti besprovodnykh setey na baze tehnologii Wi-Fi. Radioengineering, 165, 103-106.
2. Antipov, I. E., Vasilenko, T. A., Vovchenko, V. S. (2013). Primenenie teorii igr dlya zaschityi besprovodnykh wi-fi setey. Radioengineering, 173, 104-107.
3. TamoGraph Site Survey. Available at: <http://www.tamos.com>.
4. AirMagnet Planner. Available at: <http://www.keenansystems.com>.
5. Network simulation. Available at: <http://en.academic.ru>.
6. SimulationTools.bib. Available at: <http://www.idsia.ch>.
7. Proletarskiy, A. V. (2007). Besprovodnye seti Wi-Fi. BINOM. Laboratoriya znaniy, 178.
8. Dzhim, Geyer (2005). Besprovodnye seti Wi-Fi. Izdatelskiy dom «Vilyams», 192.
9. Kaspersky Security Bulletin. Razvitie ugroz v 2008 godu. Available at: <http://www.securelist.com>.
10. Shangin, V. F. (2008). Informatsionnaya bezopasnost kompyuternykh setey i sistem. ID «FSCHRUM» - INFRA-M, 416.

## ANALYZING CAPABILITIES OF QUANTUM COMPUTERS AND QUANTUM CALCULATIONS FOR CRYPTANALYSIS OF MODERN CRYPTOSYSTEMS (p. 8-16)

Yuri Gorbenko, Roman Ganzya

The main trends of the science and technology development in the field of quantum physics and quantum calculations are considered in the paper. It has been shown that over the past few years plenty of new discoveries and achievements have been made in the field of quantum physics, all these events, anyway, had a great influence on the invention and production of quantum computers. Many communities around the world have been engaged in the develop-

ment of quantum computers and some of them have achieved significant results in it by now.

It is shown that using quantum algorithms of Shor and Grover, which can be fulfilled on a properly implemented quantum computer, can compromise some symmetric and asymmetric cryptosystems. The analysis results of endurance of the known block ciphers regarding the quantum cryptanalysis are given. It is also shown that some of them are not able to resist the quantum cryptanalysis method based on Grover's algorithm.

The analysis of Shor's algorithm possibilities, which can significantly reduces computational costs for solving mathematical problems of endurance of modern asymmetric cryptoalgorithms, is given. Herewith, Shor's quantum algorithm diminishes the complexity of the cryptanalysis from exponential and subexponential to polynomial. In addition, the assessment of quantum computer resources is given in the paper, which are necessary for the quantum cryptanalysis concerning such cryptosystems as DSA, RSA, EC and NTRU

**Keywords:** quantum computer, Shor's algorithm, Grover's algorithm, quantum cryptanalysis, NTRU

### References

1. Feynman, R. (1985). Quantum mechanical computers. Opt. News, February 11., 11-39.
2. Gorbenko, I. D., Gorbenko, U. I. (2012). Applied cryptology. KNURE. Kharkov: Fort, 868.
3. Deutsch, D., Jozsa, R. (1992). Rapid Solution of problems by quantum computation. Proc. R. Soc. Lond. A. Vol. 439, 553-558.
4. Shor, P. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput., 26 (5), 1484-1509.
5. Grover, L. (1996). A fast quantum mechanics algorithm for database search Proceeding of the 28th ACM Symposium on Theory of Computation. New York: ACM Press, 212-219.
6. Perkins, R. (2012). Quantum computer built inside diamond. Futurity Research news from top universities. Available at: <http://www.futurity.org/quantum-computer-built-inside-diamond/>
7. Dalfovo, F. (1998). Theory of Bose-Einstein condensation in trapped gases Rev. Mod. Physics, 71, No 3, 463-510.
8. Heights, Y. (2012). IBM Research Advances Device Performance for Quantum Computing. IBM news. Available at: <http://www-03.ibm.com/press/us/en/pressrelease/36901.wss>
9. Geordie, R. (2012). Lockheed Martin piece about D-Wave technology. Burnaby, British Columbia, Canada, The blog of D-Wave. Available at: <http://dwave.wordpress.com/2013/03/08/lockheed-martin-piece-about-d-wave-technology/>.
10. FIPS-186-3 (2009). Digital signature standard: 2009. Gaithersburg, MD 20899-8900, 120.
11. IEEE Std 1363.1-2008 (2009). IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattice. NY: The Institute of Electrical and Electronics Engineers, Inc., 69.
12. Neven, H. (2013). Launching the quantum artificial intelligence lab. THE Blog of Google. Available at: <http://googleresearch.blogspot.ru/2013/05/launching-quantum-artificial.html>
13. Gaynutdinova, A. (2009). Quantum Computing. Kazan: Kazan State university, 272.
14. Lenstra, H., Tijdeman, Jr., Tijdeman, R. (1946). Analysis and Comparison of Some Integer Factoring Algorithms, in Computational Methods in Number Theory. Math. Centre Tract 154, 89-139.
15. Proos, J., Zalka, C. (2003). Shor's discrete logarithm quantum algorithm for elliptic curves. QIC, Vol. 4, 317-344.
16. Hoffstein, J., Silverman, J. (1998). NTRU: A ring-based public key cryptosystem. ANTS III, Vol. 1423, 267-288.
17. Silverman, J., Odlyzko, J. (2003). Meet-The Middle Attack on an NTRU Private Key. NTRU Cryptosystems: Technical Report, NTRU Report, Version 2, 7.
18. Ludwig, C. (2003). A faster lattice reduction method using quantum search. Algo Comput, Vol. 2906, 199-208.

19. Wang, X., Bao, W., Fu, X. (2010). A quantum algorithm for searching a target solution of fixed weight. *Chinese Sci Bull*, Vol. 55 (29), 484-488.
20. Xiong, Z., Wang, J., Wang, Y., Zhang, T., Chen, L. (2012). An Improved MITM Attack Against . *International Journal of Security and Its Applications*, Vol. 6, No. 2, 269-274.
21. Wang, H., Zhi, M. A., ChuanGui, M. A. (2013). An efficient quantum meet-in-the-middle attack against NTRU-2005. *Chinese Science Bulletin*, Vol. 58, No.28-29, 3514-3518.
18. Ludwig, C. (2003). A faster lattice reduction method using quantum search. *Algo Comput*, Vol.2906, 199-208.
19. Wang, X., Bao, W., Fu, X. (2010). A quantum algorithm for searching a target solution of fixed weight. *Chinese Sci Bull*, Vol. 55 (29), 484-488.
20. Xiong, Z., Wang, J., Wang, Y., Zhang, T., Chen, L. (2012). An Improved MITM Attack Against . *International Journal of Security and Its Applications*, Vol. 6, No. 2, 269-274.
21. Wang, H., Zhi, MA., ChuanGui, MA. (2013). An efficient quantum meet-in-the-middle attack against NTRU-2005. *Chinese Science Bulletin*, Vol. 58, No.28-29, 3514-3518.

### ADVANCED ALGORITHM UMAC BASED ON MODULAR TRANSFORMATIONS (p. 16-23)

Sergey Evseev, Olga Korol, Vitalii Ohurtsov

Using modular transformations allows to implement provably secure information hashing, which satisfies the collisional properties of universal hash functions. At the same time, universal hashing using modular transformations has a significant drawback - the high computational complexity of the hash code formation. In fact, it is necessary to perform modular exponentiation for each data block that significantly increases information sequence hashing time under appropriate orders of transformation module. In this regard, the development of multilayer schemes of universal hashing using modular transformations on the last and final stage of the hash code formation is a promising direction.

The selection of cycle functions in the scheme of provably secure key universal hashing is substantiated, the model and method for forming control codes of data integrity and authenticity, based on modular transformations, the algorithm for reducing the computational complexity of hashing schemes implementation using cyclic functions, are proposed in the paper. The developed advanced algorithm UMAC provides the required indicators of collisional properties of universal hashing, provable security level and high indicators of the hash code formation speed

**Keywords:** control codes of data integrity and authenticity, modular transformations, universal classes of hash functions

#### References

1. Stinson, D. R. (1988). Some constructions and bounds for authentication codes. *J. Cryptology*, 1, 37-51.
2. Stinson, D. R. (1990). The combinatorics of authentication and secrecy codes. *J. Cryptology*, 2, 23-49.
3. Kuznetsov, A. A., Korol, O. G., Evseev, S. P. (2012). Investigation of properties of conflict message authentication codes UMAC. *Applied electronics*. Kharkov: Publishing house KNURE, Vol. 11, № 2, 171-183.
4. Korol, O. G., Evseev, S. P., Parhuts, L.T. (2013). Development of a model and a method of forming a cascade MSS using modular transformations. *Zahist informatsii Naukova - tehnicny magazine*, Vol. 15, 3, 186 – 196.
5. Maitra, S., Pasalic, E. (2001). Further constructions of resilient Boolean functions with very high nonlinearity. Accepted in SETA.
6. Kuznetsov, O. O., Korol, O. G., Evseev, S. P. (2011). *Zahist informatsii in informatsiynih systems*. H. : Species . HNEU, 504.
7. Final report of European project number IST- 1999 - 12324 , named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 - Version 0.15 (beta), Springer-Verlag.
8. Stallings, W. (2001). *Cryptography and network security: Principles and Practice*, 2nd ed.: Lane. from English. Moscow: Publishing House "William", 672.
9. Korol, O. G., Evseev, S. P. (2008). Investigation of methods to ensure the authenticity and integrity of the data based on one-way hash functions. *Naukovyi - tehnicny magazine "Zahist informatsii."* Special Issue (40), 50 - 55.

10. Ischeynov, V. Y., Chudinov, S. (2012). Model security of confidential information in the information system. *Scientific statements BSU. - Publ NIU " BSU"*, Issue 23/1, 13 (132), 205 – 210.

### EXPERIMENTAL INVESTIGATION OF TIME-FREQUENCY SYNCHRONIZATION ACCURACY USING DIGITAL TELEVISION SIGNALS (p. 24-28)

Alexander Kostyria, Sergey Plehno, Vitaliy Naumenko, Sergey Ushakov

The results of studying the model of passive time-frequency synchronization system are given in the paper. The algorithm of general coverage is taken as a basis. Brief description and mathematical analysis of the algorithm of general coverage were conducted. The laboratory bench, used in this work was described. Digital terrestrial television signal is used as a general signal source. Correlation and spectral signal properties of the digital terrestrial television were shown. Sources of errors, arising in the receive and signal processing paths and their influence were estimated. An algorithm for digital processing of measurement results of scale shifts was developed. It includes spectral analysis, correlation processing, as well as mathematical methods, allowing to improve the scale difference calculation accuracy. The results of experimental investigations and their statistical analysis are shown. The graphs and bar charts, showing statistical processing results, which reflect positive trends for using the digital terrestrial television signal as a common source for comparison of time and frequency scales according to the algorithm of general coverage

**Keywords:** synchronization, standard, algorithm, digital television, error, digital processing, interpolation, zero base

#### References

1. Koval, Y., Kostyrja, A., Obelchenko, V. (2009). The analysis possibilities of the method of total enrollment for high-precision synchronization of time and frequency standards in line of sight. *Radioelektronika. Informatika. Upravlinnya. Zaporizhzhya*, № 1 (20), 21-30.
2. Koval, Y., Kostyrja, A., Obelchenko V., Cooper, E., Ivanova, E., Ermolaev E., Milyakh, M. (2009). Analysis of the possibilities of the total enrollment for high precision synchronization of time and frequency standards in a straight line. *Radioelektronika. Informatika. Upravlinnya. Zaporizhzhya*, № 2 (10), 21-30.
3. Koval, Y., Kostyrya, A., Ivanova, E., Al-Tvezhri, B. (2011). Modeling frequency-time synchronization system that use signals of common sources. *Kyiv, Radioelectronics and communication systems*, Number 2 (Vol. 54), 12-21.
4. Kundyukov, S., Kostyria, A., Koval, Y. (2010). Experimental studies of precision comparisons of time scales in the mode of zero base using signals broadcast and cable television. VII International Scientific-Technical Conference "Metrology and Measurement Techniques", 136-139.
5. Koval, Y., Kostyrja, A., Khalid-H-Asaad, Semyonov, S., Solyanik, O., Plehno, S. (2012). Selection of general signal source for regional time and frequency synchronization system. *Radioelektronika. Informatika. Upravlinnya. Zaporizhzhya*, № 2 (27), 63-69.
6. Shearman, I. (2007). *Radioelectronic systems: Fundamentals of the theory*. Moscow Radio Engineering, 512.
7. Kostyrya, A., Naumenko, V., Plehno, S., Somov, O., Khalid-H-Asaad (2013). Application of the interpolation algorithms to obtain estimates of the shift scales of time and frequency synchronization from source signals. *Radioelectronics Number 173, Kharkiv*, 88-95.
8. Rumshiskii, L. (1971). *Mathematical processing of the experimental results*. Moscow, Nauka, 192.
9. Tikhonov, V., Kharisov, V. (1991). *Statistical analysis and synthesis of wireless devices and systems*. Radio and communication, Moscow, 608.
10. Ventzel, E. (1969). *Probability theory*, Moscow, Nauka, 576.

### AUTOMATED SYSTEM OF DIAGNOSING PATHOLOGICAL CONDITIONS OF BLOOD CIRCULATORY SYSTEM (p. 29-34)

Gennady Knishov, Ievgen Nastenko, Olena Nosovets, Aleksandr Beregovii, Valentina Shapovalova, Artur Plahtyy

The results of developing an automated system of diagnosing pathological conditions of a human blood circulatory system have

been presented. The system is based on the results of researching functional bonds between arterial blood pressure measurements and cardiac rate frequency in health and disease. Nomographic charts and percentage diagrams, reflecting the type of relation depending on a blood circulatory condition, have been used. The system development has been carried out by means of the PHP programming language and implemented as a web-site.

The option of inputting results of multiple arterial blood pressure measurements for analysis allows not only estimating current blood circulation conditions, but also studying the dynamics of changes, happening to an organism under various factors (psychophysical work load, different measures aimed at eliminating pathological conditions and so on). The system provides a great range of modes: passive control (passive monitoring) of a condition domiciliary; efficiency control of measures aimed at eliminating pathological blood circulatory system conditions (surgical treatments and prescribing medicine); assessment of adaptive reserves of sportsmen; control over intraaortic balloon pump (IABP). The results of testing the system operation in different variants of its applying to clinical data have been presented

**Keywords:** blood circulatory system, arterial blood pressure, cardiac rate frequency, nomographic charts, diagnostics, pathological conditions

#### References

1. Anishchenko, O. V. (2012). Medyko – demografichna sytuatsiya ta orhanizatsiya medychnoyi dopomohy naseleennyu u 2011 rotsi. Ministerstvo okhorony zdorov'ya Ukrainy, 103.
2. Cowley, A. W., Physiolo, W. (1992). Long-term control of arterial blood pressure. *Circular Researches*, 72 (1), 231-300.
3. Euler, U. S., Liljestrand, G. (1996). Observations on the pulmonary arterial blood pressure. *Acta Physiologica Scandinavica*, 12 (4), 301–320.
4. Arthur, C., Guyton, M. D., Thomas, G. (1992). Arterial pressure regulation. *The American Journal of Medicine*, 52 (5), 584-594.
5. O'Rourke, M. (1990). Arterial stiffness, systolic blood pressure, and logical treatment of arterial hypertension. *Hypertension*, 15, 339-347.
6. McKenna, M., Wolfson, S., Kuller, L. (1991). The ratio of ankle and arm arterial pressure as an independent predictor of mortality. *Atherosclerosis*, 87 (2), 119–128.
7. McVeigh, G. E., Bratteli, C. W., Morgan, D. J. (1999). Age-Related Abnormalities in Arterial Compliance Identified by Pressure Pulse Contour Analysis. *Hypertension*, 33, 139-142.
8. Shnyrev, A. P. (2007). Osobennosti korreljatsii arterial'nogo davlenija i pokazatelej fizicheskogo razvitija. Materialy VI kongressa po detskoj nefrologii, 109.
9. Nastenka, E. A., Nosovec, E. K., Zubkov, S. V. (2011). Analiz sostojanija sistemy krovobrashhenija i mikrocirkuljatornogo rusla na osnove funkcional'nyh pokazatelej. *Biomedicinskaja inzhenerija*, 2, 42-47.
10. Knishov, G. V., Nastenko E. A., Nosovec O. K. (2012). Ocinka stanu sistemi krovoobigu za procentil'nimi digramami «vik-tisk» v gender-odnorodnih grupah. *Shhorichnik naukovih prac' Asociacii sercevo-sudinnih xipyggiv Ukraini*, 20, 230-235.
11. Winesett, J. (2012). *Web Application Development with Yii and PHP*. Packt Publishing, 332.

### CALCULATION OF ERRORS OF ULTRASONIC LOCAL POSITIONING SYSTEM (p. 34-38)

Vitaly Livnov

A high-accuracy positioning system, which for positioning uses ultrasonic waves instead of electromagnetic ones, is considered in the paper. It greatly improves the accuracy of navigation, as the sound waves have the length of several orders of magnitude less than the electromagnetic ones at the same frequencies. The system consists of ultrasonic transmitters, a base station and ultrasonic marks. The base station synchronizes ultrasonic transmitters with ultrasonic marks by means of a radio channel.

In this paper, the calculation of the mathematical model of the receiving part of an ultrasonic notch has been made that allows determining the most significant sources of system errors. The errors, caused by sound velocity vibrations, have the greatest influence on the positioning accuracy.

These vibrations are brought about by the movement of air masses (wind) or a temperature change. Another source of errors is the noise, occurring in a sound channel and generated by the system itself. Eventually, the data on error is summed up and the value increases after processing

**Keywords:** local positioning system, base station, ultrasonic transmitter, ultrasonic mark, error

#### References

1. Zhang, V. S., Parker, T. E., Weiss, M. A., Vannicola, F. M. (2000). Multi-Channel GPS/GLONASS Common-View between NIST and USNO. *EEE International Frequency Control Symposium*, 598-606.
2. Livnov, V., Koval, U. (25.05.2012). Method of ultrasonic local positioning moving objects. Patent 71860, Ukraine.
3. Livnov, V. (2011). Ultrasonic positioning system "Ultrasonic Marks" (2011). *Modern Problems of Radio Engineering and telecommunications "RT-2011": Proceedings of the 7th Intern. youth scientific and engineering. conf.*, 11-15 April 2011 – Sevastopol, SevNTU, 479.
4. Livnov, V. (2012). Ultrasonic local positioning system of moving objects 16th International Youth Forum "Radio electronics and youth in the twenty-first century. "The collection of materials. Kharkov, Vol. 3, 220.
5. Livnov, V., Koval, U. (2013). Analysis of errors and uncertainties positioning system with ultrasonic measuring and electromagnetic information channels. *Radiotekhnika: All-Ukr. Interagency, scientific and engineering collection*.
6. Parusnikov, N., Tyhomirov, V. (2005). Determination of instrument errors inertial navigation system on stationary base. *Fundamental and Applied Mathematics*, Vol. 11, № 7, 159-166.
7. Khamidullin, V. (1989). *Ultrasonic control devices and systems*. Leningrad: Leningrad University Publishing, 248.
8. Emmanuel, P. (1999). Papadakis (ed) *Ultrasonic Instruments & Devices* Academic Press.
9. Petley, B. W. (1991). Time and frequency in fundamental metrology. *PIEEE*, 1, 1070–1076.
10. Product & Service Advantage – Mathcad Available at: <http://blogs.ptc.com/product/mathcad/> – Copyright © 2013 PTC Inc.

### ESTIMATING TEMPORAL PROPERTIES OF DATA STRUCTURES AT DESIGN LEVEL (p. 39-45)

Victor Shynkarenko, Dmytro Petin, Hennadii Zabula

The approaches to estimating temporal properties of data structures without executing the program have been considered in the paper.

Temporal properties of data structures take into account the total time of data access operations during the algorithm execution. The paper considers the following approaches: direct analysis of the algorithm and a probabilistic computation of operations.

The method for determining the computational complexity of algorithms has been adapted in relation to data structures. The computational complexity of data structures is defined as the computational complexity of the combination of data processing algorithms (operations). This method should be used in programs with processing large amounts of data or with a repetitive processing.

The example of the probabilistic method of calculating operations for solving problems of the development of efficient data structures is given.

The performance evaluation of data access operations for alternative data structures is given in the paper. The evaluation of the computational complexity of the operations is carried out using combinatorial and probabilistic approaches. The obtained results are used for selecting optimal data structures

**Keywords:** data structure, computational complexity, efficiency, data operations, probability, indicators

#### References

1. Virt, N. (2010). *Algoritmy i struktury dannykh*. Moskva: DMC, 274.
2. Shinkarienko, V. I. (2009). *Ekspierimentalnye issledovaniia algoritmov v programmno-apparatnykh sriedakh*. Dnepropetrovsk: Izd-vo Dnepropietr. V. Lazarian National University of railway transport, 279.



3. Makkonniell, Dj. (2002). Analiz algoritmov. Vvodnyi kurs. Moskva: Tiekhnosfiera, 304.
4. Knut, D. (2000). Iskusstvo programmirovaniia. Tom 1. Osnovnyie algoritmy, Moskva: Izdatiiskii dom "Viliams", 720.
5. Knut, D. (2000). Iskusstvo programmirovaniia. Cortirovka i poisk. Moskva: Izdatiiskii dom "Viliams", Vol. 3, 832.
6. Kormien, T. (2001). Algoritmy: postroieniie i analiz. Moskva, 960.
7. Akho, A. (1979). Postroieniie i analiz vychislitelnykh algoritmov. Moskva: Mir, 536.
8. Akho, A. (2001). Ctruktury dannykh i algoritmy. Moskva: Izd. dom «Viliams», 384.
9. Grin, D. (1987). Matematicheskie metody analiza algoritmov. Moskva: Mir, 120.
10. Gudman, C. (1981). Vviedeniie v razrabotku i analiz algoritmov. Moskva: Mir, 366.
11. Gudrich, M.T. (2003). Ctruktury dannykh i algoritmy v Java. Minsk: Novoie znanii, 671.

### THE WAYS FOR REDUCING AGGRESSIVE INFLUENCE OF NETWORK INFORMATION RESOURCE ON USER (p. 46-50)

Denis Samoilenko

Despite the popularity of design methods on the simplification principles, still little attention has been paid to the problems of adapting these principles to the problems of network information resources design, intended for interacting with humans. A model of user's interaction with the network information resource "familiarization - comprehension - selection - action", which takes into account various stages of mental load, the level of which is suggested to consider as a complexity measure is first proposed in the paper. The factors, influencing the complexity of each interaction model phase are singled out and described, the contributions of information, semantic, combinatorial complexity, as well as selection complexity, are taken into account; the recommendations for the network information resource developer on reducing the final complexity of the developed product, defining the aggressiveness of its perception are given in the paper. The method for estimating the complexity of random information resource, allowing to determine the direction of its improvements and assess the effectiveness of the taken measures is submitted for consideration

**Keywords:** network resources, information aggression, information security, resource complexity, websites design

#### References

1. Pylypchuk, V. G. (2012). System problems of foundation and progress of IT science. Strategic priorities, 2(23), 143-148.
2. Dubov, D. V. (2012). National interests' service in information society: priorities transformation. Strategic priorities, 3(24), 120-125.
3. Nalimov, V. V. (1989). Stochastic mentality: probable theory of senses and personality architectonics. Moscow: Prometheus.
4. Pocheptsov, G. (2013). Sense and information wars: the differences. Retrieved December 10, 2012. Available at: <http://osvita.mediasapiens.ua/print/material/16366>.
5. Bourbaki, N. (2000). Worse is Better is Worse. Retrieved December 10, 2012. Available at: <http://dreamsongs.com/Files/worse-is-worse.pdf>.
6. Misra, R., Srinivasan, S, Mital, D. (2006). Outsourcing of Healthcare Services: Issues and a Framework for Success. Journal of Information Technology and Applications, 1(2), 79-88.
7. Raskin, D. (2010). Interface: new directions in computer system projection. Sankt Petersburg: Symbol-Plus.
8. Samoilenko, D. M. (2013). The methodic for task semantic complexity estimation. In Materials of scientific conference "Problems of automatics and electric equipment of transport". Mykolaiv, 19-22.
9. Fodor, J. (1998). Concepts: Where Cognitive Science Went Wrong. Oxford: Clarendon Press.
10. Velichkovskii, B. M. (2006). Cognitive science: perception psychology basics. Moscow: Academics Press.

11. Eysenck, M. & Keane, M. (2005). Cognitive Psychology (Fourth Edition). Hove and New York: Psychology Press.
12. Lomov, B. F. (Ed.). (1982). Engineer psychology directory. Moscow: Mashinostroenie.
13. Litvin, V. V., Dosin, D. G., Darevich, R. R. & Pugach, T. M. (2004). Object knowledge model in intellectual expert systems. Artificial intellect, 3, 343-349.
14. Kukol, I. I. (2013). Corporative colors usage tends in Ukrainian bank system. Retrieved January 10, 2014 from <http://bank-business-lucoz.ua/load/0-0-0-134-20>.

### EXTRACTING INFORMATION FROM SEMISTRUCTURED WEB PAGES (p. 51-54)

Andrey Kolyada, Victor Gogunsky

In most cases, information that is given on the Internet open access has no strictly-defined structure. Web pages, i.e. information sources on the Internet, can have a non-uniform layout within a resource. When it concerns the processing from such sources, there appears a problem of extracting useful information from semistructured data.

The method for solving the problem involving the so-called "web scraping" approach is proposed in the paper. The essence lies in simulating a human operation on a web resource using a low-level Hypertext Transfer Protocol (HTTP). This approach makes possible working with any data structures which become known after a preliminary data source analysis. The examples of extracting information from web pages of scientometric of a subsequent result has been developed. Further studies include the possibility of intelligent processing of extracted information to filter out irrelevant data

**Keywords:** web page, internet, information, semistructured, extraction

#### References

1. Kolyada, A., Gogunsky, V. (2013). Automating the extraction of information from scientometric databases. Management of complex systems, 16.
2. Buneman, P. (1997). Semistructured data. Proceedings of the sixteenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems, 117 – 121.
3. Burkov, V., Beloschitsky, A., Gogunsky, V. (2013). Options citation of scientific publications in scientometric databases. Management of complex systems, 15, 134 – 139.
4. Yigal, A., Chin, Y. C., Chun-Nan, H., Craig, A. K. (1993). Retrieving and integrating data from multiple information sources. International Journal of Intelligent and Cooperative Information Systems, Vol. 2, Issue 2.
5. Jane, Yung-Jen H., Wen-tau, Y. (1997). Template-based information mining from HTML documents. Proceedings of the fourteenth national conference on artificial intelligence and ninth conference on Innovative applications of artificial intelligence, 256 – 262.
6. Dan, S., Mauricio, L. (1997). Information extraction for semi-structured documents. In Proceedings of the Workshop on Management of Semistructured Data.
7. Zhao, L., Wee, K. N., Aixin, S. (2005). Web data extraction based on structural similarity. Journal Knowledge and Information Systems archive, Vol. 8, Issue 4, 438 – 461.
8. Kolyada, A., Negri, A., Kolesnikova, E. (2013). Development of the information and analytical system for extraction and processing of scientometric databases. Project management: state and prospects. International scientific conference, 9, 348.
9. Palagin, A., Kriviy, S., Petrenko, N., Bibikov, D. (2012). Formalization of the problem of knowledge extraction from natural language texts. Information technologies & knowledge, 100.
10. Baumgartner, R., Henze, N., Herzog, M. (2005). The Personal Publication Reader: Illustrating Web Data Extraction, Personalization and Reasoning for the Semantic Web. Lecture Notes in Computer Science, Vol. 3532, 515 – 530.