Evgeniya Ishchukova
PhD, Associate Professor

Date of birth: April 11, 1982
Russian nationality

Work address
Department of Information Security, SfedU
I-412, 2, Chehova st.
Taganrog, Rostov region,
Russia, 347928
Phone.:+7(8634)37-19-05
Phone/Fax:+7(8634)31-20-18
e-mail: uaishukova@sfedu.ru

Home address
Babushkina st., 57, 16
Taganrog, Rostov region,
Russia, 347909
Phone:+79281435898
e-mail: jekky82@mail.ru

Research Focus

Cryptography, Cryptanalysis, Symmetric Block Ciphers, Linear Cryptanalysis, Differential Cryptanalysis, Slide Attack, Parallel Computing.

Education

Postgraduate course (PhD)

“Methods and systems of information protection. Information Security”, Southern Federal University, Taganrog, Rostov-on-Don region, 2004-2007.

“Development and investigation of parallel algorithms for strength analysis of modern block ciphers based on differential cryptanalysis”, supervisor-Doctor of Science, Professor L.K. Babenko.

• Comprehensive exam fields:

Theory of information protection from unauthorized access;
Cryptographic mechanisms to ensure the confidentiality of information;
Cryptographic mechanisms to ensure the integrity and availability of information;
Hardware and software data protection;
Cryptographic protection of information and cryptographic algorithms;
Symmetric encryption algorithms;
Modern methods of cryptanalysis.
Parallel computing

Master of Science
(Specialist Degree in Russia)

Information Security, Southern Federal University, Taganrog, Rostov-on-Don region, 2002-2003

“Development of student practices for studying differential and linear cryptanalysis”, supervisor- Doctor of Science, Professor L.K. Babenko.

Bachelor

Information Security, Southern Federal University, Taganrog, Rostov-on-Don region, 1998-2002

“Solution of linear systems by LU decomposition using a neuro matrix processor”, supervisor- Doctor of Science, Professor L.K. Babenko.

Additional Education and Advanced Trainings

- Course “Innovative activities in education” (2008)
- Course “Multiprocessor computer systems and parallel programming” (2011).
- Course “Comprehensive protection of information facilities in educational institutions”(2012)
- Course “Modern educational technology and instructional support student learning in terms of the new generation GEF VPO of open source software” (2014)
- Course “Regulatory and scientific and methodological support of educational process in the context of practical experience in implementation of the GEF and the new generation of education in the field of information technology software” (2015)
- Course “Foreign language professionally oriented communicative competence of the teachers”(2015)
- Online Course «Cryptography I» with honor (Stanford University, Coursera Inc., 2013)

Awards, Distinctions and Fellowships

- Gold medal for the graduation from secondary school with honor, 1998;
- Potanin Scholarship to support talented youth, 2002-2003;
- The second degree diploma of the 3rd All-Russian competition of students and graduate information security «SIBINFO-2003» for the report “Cryptanalysis of speed block ciphers”, 2003;
- Diploma of the Ministry of Education on the basis of an open tender in 2003 for the best student work on natural, technical and humanitarian sciences in Russian universities, 2003;
- Governor Award of Rostov Region “Best Young Scientist”, 2008;
- Diploma “The best teacher of the Faculty of Information Security”, 2012;
- Governor Award of Rostov Region “Best Young Scientist”, 2013;
- I place in the competition “Best young scientist of Southern Federal University” in «Engineering» in the nomination “The best young scientist SFU - SFU employee”, 2015;
- Memorable badge in honor of the Day of Family, Love and Fidelity in Russia. Medal “Large family of scientists” issued by the union of the Public Chamber of the Rostov Region, the Council of Rectors of the Rostov Region, Rostov State Economic University (RINE), 2015
- Certificate for management of scientific research works for the management section “Actual problems of information security” VII International Student Research Forum 2015, The Russian Academy of Natural History, 2015.
- Award from the regional budget of the Rostov region SFU young scientists involved in research and innovation activities in 2015;
- Thanks for the contribution to the development of educational activities, SFU 2015;
- Head of the section “Actual problems of information security” within the framework of the International Student e-Scientific Conference «Student Forum» (http://www.scienceforum.ru/)

(2015-2016);

- Expert All-Russian competition of scientific and technical work of youth, 2013;
- Editor and compiler of the original layout of works of the international scientific-practical conference “Information Security” and of the All-Russian Youth School-Seminar on Information Security «PERSPECTIVA» (2007-2015);
- Member of the Organizing Committee of the Annual International Scientific and Practical Conference “Information Security”, SFU, Taganrog (2008-2015);
- Member of the Organizing Committee of the All-Russian Youth School-Seminar on Information Security «PERSPECTIVA» (2009-2016).
- Fellowship of the organizing committee on the International Conferences “Security of information and networks” (http://sinconf.org) and “Information Security” (2013-2016).
- Honorable Diploma (team competition) of the Siberian Student’s Olympiad in Cryptography with International Participation “NSUCRYPTO-2015” in category “professionals” (http://nsucrypto.nsu.ru/).
- III place diploma (team competition) of the Siberian Student’s Olympiad in Cryptography with International Participation “NSUCRYPTO-2016” in category “professionals” (http://nsucrypto.nsu.ru/).
- Scholarship of the Technical University of Darmstadt (Germany) for participation in the CrossFyre2016 conference (https://www.crossfyre2016.informatik.tu-darmstadt.de/de/the-workshop/program/)
- Honorary Diploma for achievements in the section "professionals" of the first round of the international Olympiad NSUCRYPTO-2017
- Diploma of the expert of the 1st World Skills Championship in the sphere of information technologies DigitalSlills, the competence "Blockchain-based solutions", 2017
- Diploma of the main expert of the Open University Championship of the Southern Federal University on World Skills standards, the competence " Blockchain-based solutions ", 2018
- Winner of the regional stage of the contest “My country is my Russia” in the nomination “My open universities”, 2018.
- Certificate of the chief expert of the competence “Blockchain-based solutions” of the II Open Qualifying Championship of the Southern Federal University according to WorldSkills Russia standards, 2018.
- Diploma of the winner of the All-Russian contest "My country is my Russia", 2018
- Laureate diploma of the All-Russian competition of innovative educational technologies for teachers, associate professors, professors of higher educational institutions and colleges of Russia "Best Young Teacher - 2018", 2018
- Winner diploma of the II degree of the All-Russian competition of innovative educational technologies for teachers, associate

professors, professors of higher educational institutions and colleges of Russia "Best Young Teacher - 2018" in the nomination "Best Young Teacher of Higher Education", 2018

- Letter of appreciation from the First Deputy Chairman of the Committee on Education and Science of the State Duma of the Federal Assembly of the Russian Federation Smolin O.N. for her great personal contribution to the introduction of innovative teaching technologies in the system of modern education, for the dissemination of advanced teaching practices, increasing the prestige of teaching, 2018.
- Diploma N201802 / 20 for winning the competition of university teachers "Golden Names of Higher School" in the nomination "Young scientific and pedagogical talents", 2018.
- Thanks for the help in the development and evaluation of innovative projects in the framework of the All-Russian competition of entrepreneurial projects Preactum Cup "Practices of the Future" and for their contribution to the development of youth entrepreneurship in Russia, 2019.
- Thanks for preparing and participating in the events of the 45th WorldSkills Kazan-2019 World Championship, Kazan, 2019.

Research Experience

Bachelor, Department of Information Security, Southern Federal University, Taganrog, 2001-2002
Research work: “Solution of linear systems by LU decomposition using a neuro matrix processor”
Master of Science, Department of Information Security, Southern Federal University, Taganrog, 2002-2003
“New methods of block cipher’s cryptanalysis”
Postgraduate course, Department of Information Security, Southern Federal University, Taganrog, 2004-2007
Research work: “Development and investigation of parallel algorithms for strength analysis of modern block ciphers based on differential cryptanalysis”
Assistant, Department of Information Security, Southern Federal University, Taganrog, 2003- 2008
“Cryptanalysis of asymmetric ciphers”
“Parallel computing in cryptography”
Associate Professor, Department of Information Security, Southern Federal University, Taganrog, 2008- Present
“Cryptanalysis of symmetric block ciphers”
“Cryptanalysis of hash-functions”
“Software and hardware protection of confidential information”
“Evaluation of cryptographic data protection”
Researcher, Laboratory “Fundamental problems of information security”, Institute of Computer Science and Problems of Regional Management of KBSC of the Russian Academy of Science, Nalchik, 2006 – Present
“Development and research of technology and parallel algorithms for evaluating the effectiveness of the information systems protection”
“Development and research of distributed computing methods for evaluating resistance of cryptographic algorithms based on the problems of factorization and discrete logarithm”
“Development and research of algorithms for strength analysis of modern cryptosystems using analysis methods based on the solution of linear

systems”

Grant Experience

Researcher in scientific group for grants of the Russian Foundation for Basic Research (RFBR):

- “Development and research of serial and parallel algorithms for the analysis of modern symmetric ciphers using MPI technology, NVIDIA CUDA technology, SageMath technology” (Head - Associate Professor of the Department of IS, Ph.D. Ishchukova E.A., №17-07-00654).
- “Development and research of parallel algorithms for evaluation of reliability of encryption standard GOST” (Head - Associate Professor of the Department of IS, Ph.D. Ishchukova E.A., №15-37-20007mol_a_ved).
- “Assessment of vulnerability of modern cryptographic systems using analytical methods based on solving systems of equations” (Head - Associate Professor of the Department of IS, Ph.D. Ishchukova E.A., №12-07-33007mol_a_ved);
- “Design and exploration of sequential and parallel complexity analysis algorithms applied to modern symmetric cryptography algorithms” (Head - Associate Professor of the Department of IS, Ph.D. Ishchukova E.A., №12-07-31120_mol);
- “Research and development of parallel algorithms for evaluating cryptographic protection of information” (Head - Professor of the Department of IS, Dr. Babenko L.K., №09-07-00245-a);
- “Research of reliability modern hashing functions to different methods of analysis” (Head - Professor of the Department of IS, Dr. Babenko L.K., №12-07-00037-a);
- “Development and research of algorithms of fully homomorphic encryption” (Head - Professor of the Department of IS, Dr. Babenko L.K., №15-07-00597-a);
- “Development of theory and principles of creation of system of ambient security of resources of distributed information systems on a basis of automata representation of self-organizing distributed multiagent recursive cognitive decision making systems” (Head – Director of Institute of Computer Science and Problems of Regional Management of KBSC of the Russian Academy of Science, Dr. Ivanov P.M., №13-07-01002)

Teaching Experience

Assistant:
Department of Information Security, Southern Federal University, Taganrog.

Laboratory and practical works on the courses:
“Cryptographic methods of information protection” (2003-2008).
Tutorials
“Modern methods of cryptanalysis”, 2003
“Methods of linear and differential cryptanalysis of block ciphers built on the principle of SP-network”, 2004
“Method of slide attack”, 2004
“Modern algorithms block encryption methods and analysis”, 2006
“Complex of information security tools from unauthorized access «Accord-ASGM»”, 2007
Supervisor of three student’s degree theses (2003-2008).

Associate Professor
Department of Information Security, Southern Federal University, Taganrog.

Lections on courses
“The history and modern state of information security system in Russia”(2008-2009)
“Cryptographic protocols and standards ”(2014-Present)

“Cryptographic methods of information protection” (2016-Present).

Laboratory and practical works on the courses:
“Cryptographic methods of information protection” (2008-Present).
“Technical means of protection” (2008-2009)
“Cryptographic protocols and standards ”(2014-Present)

Tutorials
“The history and modern state of data protection in Russia”, 2009
“The cryptographic methods and means of information security”, 2011
“Parallel algorithms for solving information security problems”, 2014
“Evaluation of resistance of block ciphers by the method of the slide attack”, 2015
“Cryptographic protection of information: symmetric encryption”, 2015
Supervisor of eight student’s degree theses (2008-Present).
In the future, I would like to expand my teaching courses and teach:
Cryptographic methods and means of information protection
Mathematical foundations of cryptology

Publications, Presentations and Abstracts

The results of scientific research presented in 135 publications (34 of which were published in journals recommended by Higher Attestation Commission (HAC) to present the content of master's and doctoral theses; 16 articles were included in the system of citation Scopus, also 4 monographs were published).

- Ishchukova, E., Maro, E., Pristalov, P. “Algebraic analysis of a simplified encryption algorithm GOST R 34.12-2015” // Computation. 2020
- Ishchukova, E., Salmanov, V., Kalyabin, A., Antonenko, A. “Approaches to Construct a Psychological Portrait of Users Based on Analysis of Data in Open Profiles of Social Networks” // Proceedings - 2019 1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency, SUMMA 2019
- Nissenbaum, O., Maro, E., Ishchukova, E., Zolotarev, V. “Markov and Semi-Markov Models of Real-Time Quests in Information Security Education ” // Proceedings - 2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT 2019
-
- L.K. Babenko, E.A. Ishchukova, E.A. Maro “Algebraic analysis of GOST encryption algorithm” // Proceedings of the 4th international conference on Security of information and networks (SIN 2011), ACM, New York, NY, USA, pp. 57-62.
- L.K. Babenko, E.A. Ishchukova, E.A. Maro “Research about Strength of GOST 28147-89 Encryption Algorithm” // Proceedings of the 5th international conference on Security of information and networks (SIN 2012), ACM, New York, NY, USA, pp. 80-84.
- L.K. Babenko, E.A. Ishchukova, E.A. Maro Book “Theory and Practice of Cryptography Solutions for Secure Information Systems”, Chapter “GOST Encryption Algorithm and Approaches to its Analysis”, «IGI-Global», 2013, pp. 34-61.
- Babenko L., Ishchukova E. Influence of S-Boxes to the Resistance of GOST Algorithm against Linear Cryptanalysis // Proceedings

of the 6th international conference on Security of information and networks (SIN 2013), ACM, New York, NY, USA, 132-140. (WebOfScience, DOI: 10.1145/2523514.2523557)

- L.K. Babenko, E.A. Ishchukova, E.A. Maro “Strength assessment of modern cryptosystems using methods of the analysis based on the solutions of combined equations” // International Review on Computers and Software (IRECOS), Praise Worthy Prize, Vol.
- Ishchukova, E.,Babenko, L.,Anikeev, M. Fast implementation and cryptanalysis of GOST R 34.12-2015 block ciphers // Proceedings of the 9th international conference on Security of information and networks (SIN 2016), ACM, New York, NY, USA, 104-111.10, №2 (2015) pp. 208-221.
- Ishchukova E.A., Tolomanenko E.A., Babenko L.K. Differential analysis of 3 round Kuznyechik // Proceedings of the 10th international conference on Security of information and networks (SIN 2017), ACM, New York, NY, USA. – P. 29 – 36.
- Ishchukova E.A., Babenko L.K., Anikeev M.V. Two versions of the simplified cipher Kuznyechik// Proceedings of the 10th international conference on Security of information and networks (SIN 2017), ACM, New York, NY, USA. P. 287 – 290.

Expert experience in WorldSkills competitions (competence "Blockchain-based solutions"):

- Since April 2020, a Manager of the competence "Blockchain-based solutions"
- Since November 2018, a certified expert on WorldSkills standards in the competence "Blockchain-based solutions"
- 45 World Championship WorldSkills Kazan 2019, workshop manager, chief expert;
- Foshan Future Skills Competition, China, Foshan, 2019, independent expert;
- II Open qualifying championship of the Southern Federal University according to WorldSkills Russia standards, 2018, chief expert;
- DigitalSkills qualifying competitions in the Tomsk region, 2018, chief expert;
- Qualifying Championship of NRNU MEPhI according to the standards "Young Professionals (WorldSkills Russia)", 2018, chief expert;
- Third open qualifying championship of the Southern Federal University according to Worldskills Russia standards, 2019, chief expert;
- Final of the II National Interuniversity Championship "Young Professionals (Worldskills Russia)", 2018, deputy chief expert;
- II WorldSkills industry champion in information technology DigitalSkills, 2018, deputy chief expert;
- Final of the VII National Championship "Young Professionals (Worldskills Russia)", 2019, Deputy Chief Expert.
- I WorldSkills industry champion in information technology DigitalSkills, 2017, expert.

References

Veselov Gennadiy Evgenievich
Doctor of Science, Professor

Director, Institute of computer science and information security, SFedU
e-mail: gev@tsure.ru
Tel./Fax: +7(8634) 360-450

Babenko Ludmila Klimentevna
Doctor of Science, Professor
Department of Information Security, SFedU
e-mail: blk@tsure.ru
Tel./Fax: +7(8634) 312-018

Abramov Evgenyi Sergeevich
PhD, Head of Department of Information Security, SFedU
e-mail: abramoves@sfedu.ru
Tel./Fax: +7(8634) 371-905

Anikeev Maksim Vladimirovich
PhD, Associate Professor
Department of Information Security, SFedU
e-mail: maxim.anikeev@gmail.com
Tel./Fax: +7(8634) 371-905

About myself

Married. Have 3 children: Roman (16 years old), Ivan (10 years old) and Anastasia (7 years old).
In spare time, I like to cook, travel and to craft different hand-made things.
My blog about the crafting http://ischukova.blogspot.ru/