

**Сведения об официальном оппоненте по диссертации
на соискание ученой степени кандидата технических наук
Тихонова Сергея Владимировича
«Исследование и разработка модификаций аппаратно-реализованных
защитных блоковых преобразований, устойчивых к побочным атакам
по цепям электропитания»**

Фамилия Имя Отчество: *Левина Алла Борисовна*

Гражданство: *Россия*

Место основной работы:

организация: *Университет ИТМО*

почтовый адрес: *ул. Ломоносова 9, литер M, 6 этаж 191002*

телефон: *(812) 458 43 08*

подразделение: *кафедры проектирования и безопасности
компьютерных систем*

должность: *доцент*

Учёная степень: *кандидат физико-математических наук*

по специальности *05.13.18*

Учёное звание: *доцент*

по специальности *методы и системы защиты информации,
информационная безопасность*

Основные публикации по профилю оппонируемой диссертации в научных рецензируемых изданиях за последние 5 лет (не более 15 публикаций):

1. Levina A., Taranov S. Creation of codes based on wavelet transformation and its application in ADV612 chips//International Journal of Wavelets, Multiresolution and Information Processing, 2017, Vol. 15, No. 2, pp. 1750014
2. Levina A.B., Borisenko P.S., Mostovoi R.A. Mobile Social Networking under Side-Channel Attacks: Practical Security Challenges//IEEE Access, 2017, Vol. PP, No. 99, pp. 1-10
3. Levina A.B., Taranov S.V. Investigation of influence of encoding function complexity on distribution of error masking probability//Научно-технический вестник информационных технологий, механики и оптики, 2016, Vol. 16, No. 2(102), pp. 331-337
4. Levina A.B., Taranov S.V. New Construction of Algebraic Manipulation Detection Codes Based on Wavelet Transform//Proceedings of the 18th Conference of Open Innovations Association FRUCT, 2016, pp. 187-192
5. Levina A.B., Sleptsova D., Zaitsev O. Side-Channel Attacks and Machine Learning Approach//Proceedings of the 18th Conference of Open Innovations Association FRUCT, 2016, pp. 181-186
6. Levina A.B., Borisenko P.S. Implementation of side-channel leakage detection technique based on normalized inter-class variance method//Научно-технический вестник информационных технологий, механики и оптики, 2016, Vol. 16, No. 4(104), pp. 697-702

7. Ometov A., Andreev S., Levina A., Bezzateev S. Optimizing Network-Assisted WLAN Systems with Aggressive Channel Utilization//Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2016, Vol. 9870, pp. 217-221
 8. Levina A., Taranov S. Spline-wavelet robust code under non-uniform codeword distribution//Proceedings of the 2015 3rd International Conference on Computer, Communication, Control and Information Technology, C3IT 2015, 2015, pp. 7060125
 9. Levina A.B., Taranov S.V. Algorithms of Constructing Linear and Robust Codes Based on Wavelet Decomposition and its Application//Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2015, Vol. 9084, pp. 247-258
 10. Levina A.B., Taranov S.V. Construction of Linear and Robust Codes That Is Based on the Scaling Function Coefficients of Wavelet Transforms//Journal of Applied and Industrial Mathematics, 2015, Vol. 9, No. 4, pp. 540-546
 11. Levina A.B., Taranov S.V. Second-Order Spline-Wavelet Robust Code under Non-Uniform Codeword Distribution//Procedia Computer Science, 2015, Vol. 62, pp. 297-302
 12. Levina A.B., Sleptcova D.M. Correlation Side-Channel Attack on Mifare Classic Cards//Proceedings ISPIT International Conference on Information Security and Protection of Information Technology (St.Petersburg, 5-6 November 2015), 2015, pp. 53-56
 13. Levina A.B. A New Block Ciphers Based on Wavelet Decomposition of Splines//Quasigroups and Related Systems, 2015, Vol. 23, No. 2, pp. 271-282
 14. Levina A., Korovkin M., Sleptsova D. Combined side-channel attacks on COMP128//8th IEEE International Conference on Application of Information and Communication Technologies, AICT 2014 - Conference Proceedings, 2014, pp. 7035902
 15. Levina A.B., Kuzmin I., Taranov S.V. Reed Solomon Codes and its Application for Cloud Storage System//3rd International Conference on Future Generation Communication Technologies, FGCT 2014, 2014, pp. 46-49

« 05 » 10 2017 г.

Подпись заверяю:

ПОДПИСЬ РУКИ А.Б. Левиной
Заверено: Зам. нач. упр. кадров Университета ИТМО
С.Е. Петрова
05. октября 2017г.