

Официальный оппонент по кандидатской диссертации
Березина Андрея Николаевича
на тему «Методы повышения уровня безопасности защитных преобразований
информации»

1. Фамилия, имя, отчество официального оппонента

Левина Алла Борисовна

2. Ученая степень, обладателем которой является официальный оппонент, и наименование отрасли науки, научных специальностей, по которым им защищена диссертация

Кандидат физико-математических наук по специальности 05.13.18 – «Математическое моделирование, численные методы и комплексы программ».

Отрасль науки – физико-математические науки.

3. Полное название организации, являющейся основным местом работы официального оппонента, и занимаемая им в этой организации должность

Федеральное государственное образовательное бюджетное учреждение высшего образования "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики", доцент кафедры безопасных информационных технологий

4. Список основных публикаций по теме диссертации в рецензируемых научных изданиях за последние 5 лет

1. 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. [Тип: Статья, Год: 2016]
2. Пантюхин И.С., Зикратов И.А., Левина А.Б. Метод проведения постинцидентного внутреннего аудита средств вычислительной техники на основе графов. Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 3(103). С. 506-512. [Тип: Статья, Год: 2016]
3. 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. [Тип: Статья, Год: 2016]
4. Mostovoy R., Borisenko P.S., Levina A.B. Mobile Phone Security: Side Channel Point of View. Proceedings of the 18th Conference of Open Innovations Association FRUCT. 2016. pp. 567-569. [Тип: Статья, Год: 2016]
5. Levina A.B. Optimizing Network-Assisted WLAN Systems with Aggressive Channel Utilization. Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 2016. pp. 217-221. [Тип: Статья, Год: 2016]
6. Протоколы аутентификации с нулевым разглашением секрета [Тип: Учебник, учебное пособие, Год: 2016]
7. Левина А.Б., Слепцова Д.М. Анализ атак по сторонним каналам на RFID-системы на основе протокола Mifare Classic. Вестник компьютерных и информационных технологий. 2016. № 7(145). С. 30-33. [Тип: Статья, Год: 2016]

8. Mobile Phone Security: Side Channel Point of View [Тип: Тезисы, Год: 2016]
9. 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. [Тип: Статья, Год: 2016]
10. Levina A.B., Sleptsova D., Zaitcev O.I. Side-Channel Attacks and Machine Learning Approach. Proceedings of the 18th Conference of Open Innovations Association FRUCT. 2016. pp. 181-186. [Тип: Статья, Год: 2016]
11. Левина А.Б., Пахомов А.С. Обеспечение помехоустойчивого кодирования с помощью сплайн-вейвлетных разложений. Безопасность информационных технологий. 2015. № 3. С. 91-95. [Тип: Статья, Год: 2015]
12. 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. [Тип: Статья, Год: 2015]
13. Левина А.Б., Таранов С.В. Построение линейных и надежных кодов на основе коэффициентов масштабирующих функций вейвлетных преобразований. Сибирский журнал индустриальной математики. 2015. Т. 18. № 3(63). С. 49-56. [Тип: Статья, Год: 2015]
14. 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. [Тип: Статья, Год: 2015]
15. Levina A.B., Sleptsova D. Correlation Side-Channel Attack on Mifare Classic Cards. ISPIT 2015 Conference Proceedings. 2015. pp. 53-56. [Тип: Статья, Год: 2015]
16. 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. [Тип: Статья, Год: 2015]
17. 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. [Тип: Статья, Год: 2015]
18. 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. [Тип: Статья, Год: 2015]
19. 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. [Тип: Статья, Год: 2014]
20. Левина А.Б., Коровкин М.Г. Комбинированные атаки по сторонним каналам: взлом COMP128. Безопасность информационных технологий. 2014. № 3. С. 108-112. [Тип: Статья, Год: 2014]
21. 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. [Тип: Статья, Год: 2014]