**Сведения об официальном оппоненте по диссертации на соискание ученой степени кандидата технических наук Салман Васан Давуд Салман «Разработка и исследование модели и протокола защищенной системы дистанционного электронного голосования для арабских государств с парламентской правовой системой (на опыте и примере Республики Ирак)»**

Фамилия Имя Отчество: *Левина Алла Борисовна*
Гражданство: *РФ*
Место основной работы:
организация: *федеральное государственное автономное образовательное учреждение высшего образования Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)*
ведомственная принадлежность: *Министерство науки и высшего образования Российской Федерации*
почтовый адрес: *Северо-Западный федеральный округ, субъект Российской Федерации: Санкт-Петербург, город Санкт-Петербург, ул. Профессора Попова, д. 5, лит. Б.*
телефон: *(812) 234-46-51*
подразделение: *Кафедра Информационная безопасность (ИБ)*
должность: *доцент*
Учёная степень: *кандидат физико-математических наук*
по специальности *05.13.18*
Учёное звание: *доцент*
по специальности *Методы и сиситемы защиты информации, информационная безопасность*
Академическое звание:

Основные публикации по профилю оппонируемой диссертации в рецензируемых научных изданиях, рекомендованных ВАК при Минобрнауки России, за последние 5 лет (не более 15 публикаций):

1 ) Levina A., Kadykov V., Valluri M.R. "Security Analysis of Hybrid Attack f or N T RU −Class Encryption Schemes", IEEE Access, 2023, 11, pp. 109939–109952

2) Sabbry N.H., Levina A. "Navigating through Noise Comparative Analysis of Using Convolutional Codes vs. Other Coding Methods in GPS Systems", Appl. Sci. 2023, 13, 11164

3) Levina A., Plotnikov A., "Algorithm f or simplif ying the SHA − 256 operations tree", Proceedings of the 2023 IEEE International Conference on Cyber Security and Resilience, CSR 2023, 2023, pp. 592–597

4) Levina A., Bolozovskii R., "Application of Neural Networks to Power Analysis", Engineering Proceedings. 2023; 33(1):27

5) Levina A., Ryaskin G. "Robust Code Constructions Based on Bent Functions and Spline Wavelet Decomposition", Mathematics, 2022, 10(18), 3305

6) Levina A., Mukhamedjanov D., Bogaevskiy D., Valueva M., Kaplun D. "High Performance Parallel Pseudorandom Number Generator on Cellular Automata", Symmetry, 2022, 14(9), 1869

7) Levina A., Ryaskin G. "Implementation of Spline–Wavelet Robust Bent Code in Code–Division Multiple Access", Lecture Notes in Networks and Systems, 424, 2022, pp. 479-486

8) Levina A., Ryaskin G. "Spline – wavelet bent robust codes", Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 2021, 21(6), pp. 936–941

9) Gustov V., Levina A. "Electromagnetic Fields as a Sign of Side – Channel Attacks in GSM Module", 2021 11th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2021, 2021, pp. 9432678

10) Krikun A., Levina A. "Parallelized Montgomery Exponentiation in GF (2k) f or Diffie-Hellman Key Exchange Protocol", Engineering Letters, 2021, 29(2), pp. 645–649

11) Levina, A., Ryaskin, G., Taranov, S., Polubaryeva, A. "Effectiveness of Using Codes with a Sparse Check Matrix for Protection against Algebraic Manipulations", 2021 International Conference Automatics and Informatics, ICAI 2021, 2021, pp.292-295

12) Levina, A., Varyukhin, V., Kaplun, D., Zamansky, A., van der Linden, D. "A Case Study Exploring Side – Channel Attacks On Pet Wearables", IAENG International Journal of Computer Science, 2021, 48(4), IJCS48404

13) Varuikhin, V., Levina, A. "Continuous Wavelet Transform Applications in Steganography", Procedia Computer Science, 14th International Symposium on Intelligent Systems, INTELS 2020, pp. 580–587

14) Levina A., Ryaskin G., Zikratov I. "Spline-wavelet bent robust codes, Proceedings of the 2019 Federated Conference on Computer Science and Information Systems", FedCSIS 2019, pp. 227-230

15) Levina A., Sleptsova D., Mostovoy R., Tsvetkov L., "Physical model of sensitive data leakage f rom P C – based cryptographic systems", Journal of Cryptographic Engineering - 2019, Vol. 9, No. 4, pp. 393–400

«14» декабря 2023 г. [redacted]

(подпись)

Подпись заверяется

ОТДЕЛ ПОДПИСЬ ЗАВЕРЯЮ: ЗАМ. НАЧ. ОК [redacted] М. В. СОКОЛОВА 2023