

Сведения об официальных оппонентах
по диссертации Ахметзяновой Лилии Руслановны
«Комбинаторные свойства схем обеспечения
конфиденциальности и целостности информации»

1. Ф.И.О.: Запечников Сергей Владимирович

Ученая степень: доктор технических наук

Ученое звание: доцент

Научная специальность: 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Должность: профессор отделения интеллектуальных кибернетических систем офиса образовательных программ.

Место работы: ФГБОУ ВО «Национальный исследовательский ядерный университет «МИФИ»

Адрес места работы: 115409, Москва, Каширское ш., д. 31

Тел.: +7 (495) 788-56-99

E-mail: SVZapechnikov@mephi.ru

Список основных научных публикаций по специальности 05.13.19 - методы и системы защиты информации, информационная безопасность, за последние 5 лет:

- 1) Bobrysheva J., Zapechnikov S. On the key composition for post-quantum group messaging and file exchange // Procedia Computer Science, 2021 Vol. 190, pp. 102-106.
- 2) Konkin A., Zapechnikov S. Techniques for Private Transactions in Corporate Blockchain Networks // Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021, pp. 2356-2360.
- 3) Sukhodolskiy I., Zapechnikov S. Analysis of Secure Protocols and Authentication Methods for Messaging // Procedia Computer Science, 2020, Vol. 169, pp. 407-411.
- 4) Bobrysheva J., Zapechnikov S. Post-Quantum Security of Messaging Protocols: Analysis of Double Ratcheting Algorithm // Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2020, pp. 2041-2044.
- 5) Bobrysheva J., Zapechnikov S. Post-quantum security of communication and messaging protocols: Achievements, challenges and new perspectives // Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2019, pp. 1803-1806.
- 6) Epishkina A., Zapechnikov S. On Attribute-Based Encryption for Access Control to Multidimensional Data Structures // Advances in Intelligent Systems and Computing, 2018, Vol. 636 pp. 251-256.
- 7) Kogos K., Zapechnikov S. Studying formal security proofs for cryptographic protocols // IFIP Advances in Information and Communication Technology, 2017, Vol. 503, pp. 63-73.

2. Ф.И.О.: Захаров Владимир Анатольевич

Ученая степень: доктор физико-математических наук

Научная специальность: 01.01.09 – «Дискретная математика и математическая кибернетика»

Должность: профессор кафедры математической кибернетики факультета вычислительной математики и кибернетики

Место работы: МГУ имени М.В. Ломоносова

Адрес места работы: 119991, Москва, Ленинские горы, д. 1

Тел.: +7 (495) 939-53-92

E-mail: zakh@cs.msu.ru

Список основных научных публикаций по тематике исследования за последние 5 лет:

- 1) V. A. Zakharov. Efficient equivalence checking technique for some classes of finite-state machines // Automatic Control and Computer Sciences. 2021. Т. 55. № 7. С. 670–701.
- 2) А. Р. Гнатенко, В. А. Захаров. О верификации моделей и проверке выполнимости формул одного параметрического расширения темпоральной логики линейного времени // Моделирование и анализ информационных систем. 2021. Т. 28. № 4. С. 378–393.
- 3) Е. М. Vinarskii, V. A. Zakharov. On some properties of timed finite state machines. // Системная информатика. 2020. Т. 17. С. 11-20.
- 4) В. А. Захаров. Эффективные алгоритмы проверки эквивалентности для некоторых классов автоматов. // Моделирование и анализ информационных систем. 2020. Т. 27. № 3. С. 260-303.
- 5) М. М. Аббас, Н. П. Варновский, В. А. Захаров, А. В. Шокуров. О дедуктивной безопасности запросов к базам данных с многобитовыми записями // Вестник Московского университета. 2019. Т. 15. № 1. С. 40–45.
- 6) А. В. Шокуров, И. В. Абрамова, Н. П. Варновский, В. А. Захаров. О возможности стойкой обфускации программ в одной модели облачных вычислений // Труды Института

3. Ф.И.О.: Шишкин Василий Алексеевич

Ученая степень: кандидат физико-математических наук

Научная специальность: 20.03.04 – «Теоретическая криптография»

Должность: руководитель лаборатории криптографии

Место работы: АО «НПК «Криптонит»

Адрес места работы: 115114, Москва, Шлюзовая набережная, д. 4

Тел.: +7 (499) 455 04 13

E-mail: v.shishkin@kryptonite.ru

Список основных научных публикаций по тематике исследования за последние 5 лет:

- 1) V. Lavrikov, V. A. Shishkin, “How much data may be safely processed on one key in different modes?” // Математические вопросы криптографии. 2019. Т. 10. № 2. С. 125-134.
- 2) D. V. Denisenko, G. B. Marshalko, M. V. Nikitenkova, V. I. Rudskoi, and V. A. Shishkin. Estimating the complexity of grover’s algorithm for key search of block ciphers defined by GOST R 34.12-2015. // Journal of Experimental and Theoretical Physics. 2019. Т. 128. № 4. С. 552–559.
- 3) Vladimir Belsky, Ivan Chizhov, Anastasiya Chichaeva, Vasily Shishkin. Physically Unclonable Functions in cryptography // International Journal of Open Information Technologies. 2020. Т. 8. № 10. С. 10-26.
- 4) Ekaterina Griboedova, Vasily Shishkin. Not so long, but very rich: a history of Russian crypto standardization // J. Comput. Virol. Hacking Tech. 2020. Т. 16. № 4. С. 261-264.
- 5) С.А. Давыдов, В.А. Шишкин. Разложение рекурсивных матриц и его применение к реализации XSL-схем // Proceedings of the XXIII conference RusCrypto, 2021.
- 6) С.А. Давыдов, В.А. Шишкин. Использование преобразований, задаваемых умножением на элемент кольца, в качестве линейных преобразований в XSL-схемах // Proceedings of the XXIV conference RusCrypto, 2022.

Ученый секретарь

диссертационного совета МГУ.05.01

к.ф.-м.н.

М.А. Кривчиков