Сведения об официальных оппонентах
по диссертации *Бабуевой Александры Алексеевны*
«Свойства безопасности схем подписи вслепую на основе уравнений Шнорра и Эль-Гамаля»

1. Ф.И.О.: Нестеренко Алексей Юрьевич
Ученая степень: доктор физико-математических наук
Ученое звание:
Научная специальность: 2.3.6 – «Методы и системы защиты информации, информационная безопасность»
Должность: профессор
Место работы: ФГАОУ ВО "Национальный исследовательский университет "Высшая школа экономики", кафедра компьютерной безопасности Московского института электроники и математики им. А.Н. Тихонова
Адрес места работы: 109028, Россия, Москва, Покровский бульвар, д.11
Тел.: +7 (495) 772-95-90 доб. 15125
E-mail: anesterenko@hse.ru

Список основных научных публикаций по специальности(тям) и/или проблематике оппонируемой диссертации за последние 5 лет:

1. Нестеренко А.Ю. Семенов А.М. Методика оценки безопасности криптографических протоколов // Прикладная дискретная математика, 2022, № 56, 33–82
2. Nesterenko A. Differential properties of authenticated encryption mode based on universal hash function (XTSMAC) // 2021 XVII International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY). Ed. by E. Krouk. IEEE, 2021, p.39-44.
3. Nesterenko A., Semenov A. On the practical implementation of Russian protocols for low-resource cryptographic modules // Journal of Computer Virology and Hacking Techniques. 2020. Vol. 16. No. 4. P. 305–312.
4. Нестеренко А. Ю., Семенов А. М. Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств // Безопасность информационных технологий. 2020. Т. 27. № 4. С. 7–16.

2. 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
Место работы: ФГАОУ ВО "Национальный исследовательский ядерный университет "МИФИ", кафедра криптологии и кибербезопасности Института интеллектуальных кибернетических систем
Адрес места работы: 115409, Россия, Москва, Каширское шоссе, 31

Тел.: +7(495)788-56-99, доб. 91-46
E-mail: SVZapechnikov@mephi.ru

Список основных научных публикаций по специальности(тям) и/или проблематике оппонируемой диссертации за последние 5 лет:

1. Шевченко В.А., Запечников С.В. Обеспечение конфиденциальности применения предварительно обученных графовых нейронных сетей с механизмом внимания // Вопросы кибербезопасности, 2024. - Вып. 5. - С. 18-27.
2. Афонин В.Д., Запечников С.В., Простов И.А. Анализ возможностей применения алгоритма ГОСТ 34.11-2018 в системах доказательства с нулевым разглашением // Безопасность информационных технологий, 2024. - Т. 31, Вып. 2. - С. 81-89.
3. Запечников С.В., Конкин А.Ю. Обеспечение конфиденциальности информации в системах распределенного реестра посредством доказательств с нулевым разглашением // Безопасность информационных технологий, 2024. - Т. 31, Вып. 1. - С. 75-85.
4. Konkin A., Zapechnikov S. Systematization of knowledge: privacy methods and zero knowledge proofs in corporate blockchains // Journal of Computer Virology and Hacking Techniques, 2024. – Vol. 20. – Pp. 219-224.
5. Konkin A., Zapechnikov S. Zero knowledge proof and ZK-SNARK for private blockchains // Journal of Computer Virology and Hacking Techniques, 2023. – Vol. 19. – Pp. 443-449.

3. Ф.И.О.: Коренева Алиса Михайловна
Ученая степень: кандидат физико-математических наук
Ученое звание:
Научная(ые) специальность(и): 05.13.19 – «Методы и системы защиты информации, информационная безопасность»
Основное место работы: ООО «Код безопасности»
Должность: заместитель руководителя службы сертификации по научно-техническому сотрудничеству
Адрес: 115230, Россия, Москва, 1-й Нагатинский проезд, д. 10, стр. 1
Второе место работы: Финансовый университет при Правительстве Российской Федерации
Должность: доцент департамента ИБ
Адрес: 125167, Россия, Москва, пр-кт Ленинградский, д. 49/2.
Тел.: +7 (903) 290-29-12
E-mail: A.Koreneva@securitycode.ru

Список основных научных публикаций по специальности(тям) и/или проблематике оппонируемой диссертации за последние 5 лет:

1. Fomichev V., Bobrovskiy D., Koreneva A., Nabiev T., Zadorozhny D. Data integrity algorithm based on additive generators and hash function //Journal of Computer Virology and Hacking Techniques. – 2022. – Т. 18. – №. 1. – С. 31-41.
2. Firsov G. V., Koreneva A. M. On Improving Performance of One Block Ciphers Mode of Operation Used for Protection of Block-Oriented System Storage Devices //International Journal of Open Information Technologies. – 2024. – Т. 12. – №. 9. – С. 84-92.
3. Firsov G., Koreneva A. On improved security bounds of one block ciphers mode of operation for protection of block-oriented system storage devices //Journal of Computer Virology and Hacking Techniques. – 2024. – Т. 20. – №. 3. – С. 513-523.
4. Firsov G., Koreneva A. On post-quantum security properties of one block ciphers mode of operation for block-oriented storage devices protection //Journal of Computer Virology and Hacking Techniques. – 2025. – Т. 21. – №. 1. – С. 12.
5. Firsov G., Koreneva A. Correction to: On improved security bounds of one block ciphers mode of operation for protection of block-oriented system storage devices //Journal of Computer Virology and Hacking Techniques. – 2025. – Т. 21. – №. 1. – С. 19.

Ученый секретарь
диссертационного совета МГУ.012.3,
А. В. Галатенко