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: *Александрова Елена Борисовна*
Гражданство: *Российская Федерация*
Место основной работы:
организация: *федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого»*
ведомственная принадлежность: *Министерство науки и высшего образования Российской Федерации*
почтовый адрес: *195251, г.Санкт-Петербург, ул.Политехническая, 29*
телефон: *(812) 552-76-32*
подразделение: *Высшая школа кибербезопасности*
должность: *Профессор*
Учёная степень: *доктор технических наук*
по специальности *2.3.6. Методы и системы защиты информации, информационная безопасность*
Учёное звание: *доцент*
по кафедре *информационной безопасности компьютерных систем*
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. Александрова, Е. Б. Протокол с нулевым разглашением для управления отзывами на товары и услуги / Е. Б. Александрова, В. С. Шматов // Проблемы информационной безопасности. Компьютерные системы. - 2019. - № 1. - С. 31-40.

2. Александрова, Е. Б. Организация отзыва для схемы цифровой подписи / Е. Б. Александрова, И. В. Рехвиашвили // Проблемы информационной безопасности. Компьютерные системы. - 2019. - № 2. - С. 80-85.

3. Александрова, Е. Б. Отзыв со связыванием в схеме кольцевой подписи на решетках для промышленного интернета вещей / Е. Б. Александрова, И. Ш. Рехвиашвили, А. В. Ярмак // Проблемы информационной безопасности. Компьютерные системы. - 2020. - № 1. - С. 50-57.

4. Александрова, Е. Б. Аутентификация управляющих устройств в сети интернета вещей с архитектурой граничных вычислений / Е. Б. Александрова, А. Ю. Облогина, Е. Н. Шкоркина // Проблемы информационной безопасности. Компьютерные системы. - 2021. - № 2. - С.82-88.

5. Александрова, Е. Б. Иерархическая групповая аутентификация для защищенного взаимодействия узлов в промышленном Интернете вещей /

Е. Б. Александрова, А. В. Ярмак // Защита информации. Инсайд. - 2021. - № 2 (98). - С. 23-27.

6. Костин, С. О. Исследование структуры графа изогений суперсингулярных кривых для протоколов постквантовой криптографии / С. О. Костин, Е. Б. Александрова // Проблемы информационной безопасности. Компьютерные системы. - 2023. - № S2 (55). - С. 183-193.

7. Aleksandrova, E. B. Analysis of Approaches to Group Authentication in Large-Scale Industrial Systems / E. B. Aleksandrova, A. V. Yarmak, M. O. Kalinin // Automatic Control and Computer Sciences. - 2019. - Т. 53. - № 8. - С. 879-882.

8. Aleksandrova, E. B. Post-Quantum Primitives in Information Security / E. B. Aleksandrova, A. A. Shtyrkina, A. V. Iarmak // Nonlinear Phenomena in Complex Systems. - 2019. - Т. 22. - № 3. - С. 269-276.

9. Aleksandrova, E. B. Post-quantum group-oriented authentication in IoT / E. B. Aleksandrova, A. A. Shtyrkina, A. V. Yarmak // Nonlinear Phenomena in Complex Systems. - 2020. - Vol. 23. - No 4. - P. 405-413.

10. Aleksandrova, E. B. Isogeny-Based Cryptographic Access Control / E. B. Aleksandrova, A. A. Shtyrkina, A. V. Yarmak // Automatic Control and Computer Sciences. - 2020. - Vol. 54. - No. 8. - P. 803-812.

11. Aleksandrova, E. B. Ensuring the Big Data integrity through verifiable zero-knowledge operations / E. B. Aleksandrova, M. A. Poltavtseva, V. S. Shmatov // Communications in Computer and Information Science. - 2022. - Т. 1544. - С. 211-221.

12. Aleksandrova, E. Threshold Isogeny-Based Group Authentication Scheme / E. Aleksandrova, O. Pendrikova, A. Shtyrkina, E. Shkorkina, A. Yarmak, J. Tick // Lecture Notes in Networks and Systems. - 2022. - Т. 387. - С. 117-126.

13. Александрова, Е. Б. Программа для поддержания доверенного взаимодействия функциональных узлов в иерархических киберсредах / Е. Б. Александрова, А. В. Ярмак // Свидетельство о регистрации программы для ЭВМ RU 2022680367, 31.10.2022.

14. Шкоркина, Е. Н. Программа для оценки эффективности применения двойного делегирования вычислений в протоколах аутентификации и защищенного управления в граничной архитектуре / Е. Н. Шкоркина, Е. Б. Александрова // Свидетельство о регистрации программы для ЭВМ RU 2023668460, 28.08.2023.

15. Ярмак, А. В. Программа для моделирования протоколов иерархической аутентификации данных на основе схемы CSI-FISH / А. В. Ярмак, Е. Б. Александрова // Свидетельство о регистрации программы для ЭВМ RU 2023668009, 22.08.2023.

«19» декабря 2023 г. [redacted]

(подпись)

[redacted]

Александрова Е.Б.

ЗАВЕРЯЮ

[redacted]

19.12.2023 г.