

Сведения об официальных оппонентах
по диссертации Матвеева Евгений Анатольевича
«Применение квантовомеханических эффектов в системах защиты информации»

1. Ф.И.О.: Кулик Сергей Павлович

Ученая степень: доктор физико-математических наук

Ученое звание: профессор

Научная специальность: 01.04.21 – «Лазерная физика»

Должность: профессор кафедры квантовой электроники Физического факультета МГУ им. М.В. Ломоносова

Место работы: Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М. В. Ломоносова»

Адрес места работы: 119991, Москва, Ленинские горы, МГУ им. М.В. Ломоносова, физический факультет, кафедра квантовой электроники

Тел.: +7 (495) 939-11-04

E-mail: skulik@qopt.phys.msu.su

Список основных научных публикаций по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» за последние 5 лет:

1. Katamadze K.G., Kovlakov E.V., Avosopiants G.V., Kulik S.P. Direct test of the «quantum vampire's» shadow absence with use of thermal light // Optics Letters. – 2019. – V. 44. – no 13. – P. 3286.

2. Porozova V.M., Gerasimov L.V., Bobrov I.B., Straupe S.S., Kulik S.P., Kupriyanov D.V. Raman sideband cooling of a single atom in an optical dipole trap: towards theoretical optimum in a three-dimensional regime // Physical Review A - Atomic, Molecular, and Optical Physics. – 2019. – Vol. 99. – P. 043406.

3. Struchalin G.I., Kovlakov E.V., Straupe S.S., Kulik S.P. Adaptive quantum tomography of high-dimensional bipartite systems // Physical Review A - Atomic, Molecular, and Optical Physics. – 2018. – Vol. 93. – no. 3. – P. 032330.

4. Balygin K.A., Klimov A.N., Bobrov I.B., Kravtsov K.S., Kulik S.P., Molotkov S.N. Inherent security of phase coding quantum key distribution systems against detector blinding attacks // Laser Physics Letters. – 2018. – Vol. 15. – No. 5. – P. 095203.

5. Kovlakov E.V., Straupe S.S., Kulik S.P. Quantum state engineering with twisted photons via adaptive shaping of the pump beam // *Physical Review A - Atomic, Molecular, and Optical Physics*. – 2018. – Vol. 98. – No. 6. – P. 060301.

6. Kravtsov K.S., Radchenko I.V., Kulik S.P., Molotkov S.N. Relativistic quantum key distribution system with one-way quantum communication // *Scientific reports*. – 2018. – Vol. 8. – P. 1-7.

2. Ф.И.О.: Аблаев Фарид Мансурович

Ученая степень: доктор физико-математических наук

Ученое звание: профессор

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

Должность: заведующий кафедрой теоретической кибернетики Института вычислительной математики и информационных технологий Казанского федерального университета

Место работы: Федеральное государственное автономное образовательное учреждение высшего образования «Казанский (Приволжский) федеральный университет»

Адрес места работы: 420008, Казань, Кремлевская, 35, к.902,908

Тел.: +7 (843) 233-70-48

E-mail: farid.ablayev@kpfu.ru

Список основных научных публикаций по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» за последние 5 лет:

1. Ablayev F.M.; Andrianov S. N.; Vahrushev D. V.; Ziatdinov M. T.; Romanov V. S.; Soloviev A. A. Robust random number generator based on field effect transistor Proceedings of SPIE - The International Society for Optical Engineering. – 2019. – Vol. 11022. – P. 1102229.

2. Ablayev F.M., Bulychkov D.A., Sapaev D.A., Vasiliev A.V., Ziatdinov M.T. Quantum-assisted blockchain // *Lobachevskii Journal of Mathematics*. – 2018. – Vol. 39. – no. 7. – P. 957-960.

3. Ablayev F., Fetisov D., Terentyev A., Urmanchev A., Vasiliev A., Andrianov S., Moiseev S. Model of a programmable quantum processing unit based on a quantum transistor effect // *AIP Conference Proceedings*. – 2018. – P. 020014.

4. Ablayev F., Ablayev M., Vasiliev A. Computing quantum hashing in the model of quantum branching programs // *AIP Conference Proceedings*. – 2018. – P. 020020.

5. Ablayev F., Gainutdinova A., Khadiev K., Yakaryılmaz A. Very narrow quantum OBDDs and width hierarchies for classical OBDDs // Lobachevskii Journal of Mathematics. – 2016. – Vol. 37. – no. 6. – P. 670-682.

6. Аблаев Ф.М., Аблаев М.Ф. О понятии квантового хеширования // Математические вопросы криптографии. – 2016. – Т. 7. – № 2. – С. 7-20.

3. Ф.И.О.: Баранов Александр Павлович

Ученая степень: доктор физико-математических наук

Ученое звание: старший научный сотрудник

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

Должность: зам. Генерального директора АО «Главный научный инновационный вычислительный центр» (ГНИВЦ)

Место работы: АО «Главный научный инновационный вычислительный центр» (ГНИВЦ)

Адрес места работы: 125373, г. Москва, Походный проезд, домовладение 3, стр.1

Тел.: +7 (495) 913-19-63

E-mail: info@gnivc.ru

Список основных научных публикаций по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» за последние 5 лет:

1. Баранов А.П., Баранов П.А. Оценка вероятности ошибки контрольной суммы в сообщении // Проблемы информационной безопасности. Компьютерные системы. 2018. – № 4. – С. 62-67.

2. Баранов А.П., Баранов П.А. Модели образования значений сгси контрольных сумм в условиях множественных искажений // Проблемы информационной безопасности. Компьютерные системы. – 2017. – № 2. – С. 39-45.

3. Баранов А.П., Баранов П.А. Вероятность ошибки CRC при наличии пакетной случайной помехи // Проблемы информационной безопасности. Компьютерные системы. – 2017. – № 4. – С. 113-121.

4. Baranov A.P., Baranov P.A. Models of the formation of CRC values and monitoring sums under the conditions of multiple distortions // Automatic Control and Computer Sciences. 2017. – Vol. 51. – no. 8. – P. 959-964.

5. Баранов А.П., Баранов П.А. Асимптотические оценки вероятностей ошибок CRC в некоторых телекоммуникационных протоколах // Проблемы

информационной безопасности. Компьютерные системы. – 2016. – № 1. – С. 70-75.

6. Баранов А.П., Баранов П.А. Оценка вероятности ошибки CRC при малом искажении передаваемой информации // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 2. – С. 80-89.

Ученый секретарь
диссертационного совета
МГУ.05.01
к. ф.-м. н.

М. А. Кривчиков