**Сведения об официальных оппонентах**

**по диссертации Нестеренко Алексея Юрьевича**

**«Математические методы обеспечения защищенного взаимодействия средств защиты информации»**

**1. Ф.И.О.: Алиев Физули Камилович**

**Ученая степень:** д.ф.-м.н.

**Ученое звание:** доцент

**Научная(ые) специальность(и):** 05.13.19 «Методы и системы защиты информации, информационная безопасность»

**Должность:** департамент информационных систем, консультант

**Место работы:** Министерство обороны Российской Федерации

**Адрес места работы:** г. Москва

**E-mail:** alievfk@mail.ru

1. Математические основы применения квантовой фотонной компьютерной технологии решения сложных вычислительных задач систем высокой доступности / Ф. К. Алиев, А. П. Баранов, А. В. Ивахин [и др.] // Системы высокой доступности. – 2023. – Т. 19, № 1. – С. 14-27. – doi: 10.18127/j20729472-202301-02.

2. Алиев, Ф. К. Класс квантовых криптографических систем АКМ2021 на основе использования синглетных состояний многокубитовых квантовых систем / Ф. К. Алиев, А. В. Корольков, Е. А. Матвеев // Системы высокой доступности. – 2022. – Т. 18, № 3. – С. 5-22. – doi: 10.18127/j20729472-202203-01.

3. Квантовая фотонная компьютерная технология решения сложных вычислительных задач систем высокой доступности / Ф. К. Алиев, Е. Г. Букин, А. В. Корольков, Е. А. Матвеев // Системы высокой доступности. – 2021. – Т. 17, № 4. – С. 34-54. – DOI 10.18127/j20729472-202104-03.

4. О чувствительности гаммы квантовой криптографической системы АКМ2017 к изменениям сеансового ключа / Ф. К. Алиев, А. В. Корольков, Е. А. Матвеев, И. А. Шеремет // Программная инженерия. – 2021. – Т. 12, № 4. – С. 179-188. – DOI 10.17587/prin.12.179-188.

**2. Ф.И.О.: Логачев Олег Алексеевич**

**Ученая степень:** д.ф.-м.н.

**Ученое звание:** доцент

**Научная(ые) специальность(и):** 05.13.19 «Методы и системы защиты информации, информационная безопасность»

**Должность:** доцент кафедры информационной безопасности факультета вычислительной математичеки и кибернетики МГУ им. М.В. Ломоносова

**Место работы:** ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова»

**Адрес места работы:** г. Москва

**E-mail:** logol@iisi.msu.ru

1. А. А. Бабуева, О. А. Логачев, В. В. Ященко. О связи локальных аффинностей булевой функции с некоторыми видами ее вырожденности // Дискретная математика, 34:2 (2022), С. 7–25. – doi: 10.4213/dm1707.

2. О. А. Логачев, С. Н. Федоров, В. В. Ященко. О некоторых инвариантах действия расширения GA(n,2) на множестве булевых функций // Дискрет. матем., 33:2 (2021), С. 66–85. - doi: 10.1515/dma-2022-0016.

3. О. А. Логачев, А. А. Сукаев, С. Н. Федоров. Об одном методе решения систем квадратичных булевых уравнений, использующем локальные аффинности // Информация и её применения, 13:2 (2019), 37–46. - doi: 10.14357/19922264190206.

4. О. А. Логачев, А. А. Сукаев, С. Н. Федоров. Полиномиальные алгоритмы вычисления локальных аффинностей квадратичных булевых функций // Информация и её применения, 13:1 (2019), 67–74. - doi: 10.14357/19922264190110.

**3. Ф.И.О.:** Смышляев Станислав Витальевич

**Ученая степень:** д.ф.-м.н.

**Ученое звание:**

**Научная(ые) специальность(и):** 05.13.19 «Методы и системы защиты информации, информационная безопасность»

**Должность:** заместитель генерального директора

**Место работы:** ООО «КРИПТО-ПРО»

**Адрес места работы:** г. Москва

**E-mail:** svs@cryptopro.ru

1. Alekseev, E., Kyazhin, S., Smyshlyaev, S. The threat of forcing the identical roles for authenticated key establishment protocols. J. Comput. Virol. Hack. Tech. (2023). https://doi.org/10.1007/s11416-023-00471-4.

2. L. R. Akhmetzyanova, E. K. Alekseev, A. A. Babueva, L. O. Nikiforova, S.V. Smyshlyaev. IQRA: Incremental Quadratic Re-keying friendly Authentication scheme // Математические вопросы криптографии, 13:3 2022. P. 5–35. - doi: 10.4213/mvk413.

3. Смышляев С.В. Влияние рандомизации в механизмах VKO на безопасность средств защиты информации / Алексеев Е.К., Николаев В.Д., Смышляев С.В. // Прикладная дискретная математика. 2021. № 4 (54). С. 78–94. - doi: 10.17223/20710410/54/3.

4. Смышляев С.В. О повышении безопасности схем подписи ЭльГамаля / Алексеев Е.К., Ахметзянова Л.Р., Бабуева А.А., Смышляев С.В. // Математические вопросы криптографии. 2021. Т. 12. No 3. С. 5–30. doi: 10.4213/mvk373.

5. Е. К. Алексеев, С. В. Смышляев. О безопасности протокола SESPAKE // Прикладная дискретная математика. 2020, № 50, 5–41. - doi: 10.17223/20710410/50/1.

Ученый секретарь

диссертационного совета МГУ.012.3

к.ф.-м.н. Галатенко А.В.