Сведения об официальных оппонентах
по диссертации Чередника Игоря Владимировича
«Использование бинарных функциональных сетей при построении кратно транзитивных множеств блочных преобразований»

Ф.И.О.: Логачев Олег Алексеевич
Ученая степень: д.ф.-м.н.
Ученое звание: без звания
Должность: ведущий научный сотрудник
Место работы: Институт проблем информационной безопасности (ИПИБ МГУ)
Адрес места работы: 119192, Москва, Мичуринский проспект, д. 1, НИИ механики МГУ
Тел: +7 (495) 932-89-58
E-mail: ollog@inbox.ru

Список основных научных публикаций по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки) за последние 5 лет:

1. *Логачев О. А., Федоров С. Н., Ященко В. В.* О некоторых инвариантах действия расширения *GA(n,2)* на множестве булевых функций // *Дискрет. матем.* — 2021. — Том 33, № 2. — С. 66–85.

2. *Логачев О. А., Сукаев А. А., Федоров С. Н.* Об одном методе решения систем квадратичных булевых уравнений, использующем локальные аффинности // *Информ. и ее примен.* — 2019. — Том 13, № 2. — С. 37–46.

3. *Логачев О. А., Сукаев А. А., Федоров С. Н.* Полиномиальные алгоритмы вычисления локальных аффинностей квадратичных булевых функций // Информ. и ее примен. — 2019. — Том 13, № 1. — С. 67–74.

4. *Логачев О. А., Федоров С. Н., Ященко В. В.* О Δ-эквивалентности булевых функций // *Дискрет. матем.* — 2018. — Том 30, № 4. — С. 29–40.

5. *Логачев О. А., Федоров С. Н., Ященко В. В.* Булевы функции как точки на гиперсфере в евклидовом пространстве // *Дискрет. матем.* — 2018. — Том 30, № 1. — С. 39–55.

6. *Логачев О. А.* Теоретико-информационная характеризация совершенно уравновешенных функций // *Информ. и ее примен.* — 2018. — Том 12, № 4. — С. 70–74.

7. *Alekseev E. K., Karelina E. K., Logachev O. A.* On construction of correlation-immune functions via minimal functions // *Матем. вопр. криптогр.*— 2018.— Том 9, № 2.— С.7-22.

8. *Логачев О. А.* О локальной обратимости конечных автоматов без потери информации // *Прикладная дискретная математика.* — 2018. — № 39. — С. 78–93.

9. *Логачев О. А.* Критерий совершенной уравновешенности сдвиг-композиции над конечным алфавитом // *Дискрет. матем.* — 2017. — Том 29, № 4. — С. 59–65.

Ф.И.О.: Пудовкина Марина Александровна
Ученая степень: д.ф.-м.н.
Ученое звание: без звания
Должность: профессор отделения интеллектуальных кибернетических систем офиса образовательных программ
Место работы: Национальный исследовательский ядерный университет «МИФИ»
Адрес места работы: 115409, Москва, Каширское ш., 31
Тел: +7 (495) 788-56-99
E-mail: mapudovkina@mephi.ru

Список основных научных публикаций по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки) за последние 5 лет:

1. *Gorodilova A.A., Tokareva N.N., Agievich S.V., Carlet C., Gorkunov E.V., Idrisova V. A., Kolomeec N.A., Kutsenko A.V., Lebedev R.K., Nikova S., Oblaukhov A.K., Pankratova I.A., Pudovkina M. A., Rijmen V., Udovenko A.N.* On the Sixth International Olympiad in Cryptography NSUCRYPTO // *J. Appl. Industr. Math.* — 2020. — V.14, № 4, pp. 623–647.

2. *Погорелов Б. А., Пудовкина М. А.* Неабелевость группы наложения ключа и свойство $\otimes_W$-марковости алгоритмов блочного шифрования // *Матем. вопр. Криптогр.* — 2020. — Том 11, № 4 — С. 107–131.

3. *Sorokin M., Pudovkina M.* On Integral Distinguishers for Ciphers Based on the Feistel Network Generalizations // *Mechanisms and Machine Science.* — 2020. — Vol. 80, Q4. — pp. 189-197.

4. *Погорелов Б.А., Пудовкина М.А.* Характеризация отображений через свойство неизометричности // *Матем. вопр. криптогр.* — 2019. — Том 10, № 4 — С. 77–116.

5. *Погорелов Б.А., Пудовкина М.А.* Классификация дистанционно транзитивных графов орбиталов надгрупп группы Джевонса // *Дискрет. матем.* — 2018. — Том 30, № 4. — С. 66–87.

6. *Погорелов Б.А., Пудовкина М.А.* Разбиения на биграммах и марковость алгоритмов блочного шифрования // *Матем. вопр. криптогр.* — 2017. — Том 8, № 1. — С. 107–142.

7. *Pogorelov B.A., Pudovkina M.A.* Orbital derivatives over subgroups and their combinatorial and group-theoretic properties // *Discrete Mathematics and Applications.* — 2016. — V. 26. — № 5. — pp. 279-298.

8. *Погорелов Б.А., Пудовкина М.А.* О группах, содержащих аддитивную группу кольца вычетов или векторного пространства // *Дискрет. матем.* — 2016. — Том 28, № 4. — С. 100–121.

Ф.И.О.: Афонин Сергей Александрович
Ученая степень: к.ф.-м.н.
Ученое звание: без звания
Должность: ведущий научный сотрудник
Место работы: НИИ механики МГУ имени М.В. Ломоносова
Адрес места работы: 119192, Москва, Мичуринский проспект, д. 1, НИИ механики МГУ, 404 Лаборатория автоматизации экспериментальных исследований
Тел: +7 (495) 939-53-06
E-mail: serg@msu.ru

Список основных научных публикаций по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки) за последние 5 лет:

1. *Афонин С. А., Кузнецова А. Л.* Автоматная модель проверки корректности атрибутной политики информационной безопасности в системах с конечным числом объектов // *Вестник Московского университета. Серия 1: Математика. Механика*. — 2021. — № 5. — С. 57–60.

2. *Афонин С. А., Бонюшкина А. Ю.* Анализ атрибутивной политики безопасности с использованием методов автоматического планирования // *Интеллектуальные системы. Теория и приложения*. — 2020. — Т. 24, № 4. — С. 7–31.

3. *Afonin S., Bonushkina A.* Validation of safety-like properties for entity-based access control policies // Proc. of the international conference Advances in Soft and Hard Computing. — Vol. 889 of *Advances in Intelligent Systems and Computing*. — Springer International Publishing, 2019. — P. 259–271.

4. *Afonin S.* Decision problems and applications of rational sets of regular languages // *Fundamenta Informaticae*. — 2018. — Vol. 162, №. 2-3. — P. 101–118.

5. *Afonin S.* Ontology models for access control systems // Proc. of the 3rd International Conference Russian-Pacific Conference on Computer Technology and Applications (RPC). — 2018. — P. 1–6.

6. *Afonin S.* Performance evaluation of a rule-based access control framework // MIPRO 2016 - 39th International Convention. — 2016. — P. 1656–1662.

Ученый секретарь
диссертационного совета МГУ.05.01
М. А. Кривчиков