

Сведения о научном консультанте
 по диссертации Пудовкиной Марины Александровны
 «Комбинаторно-алгебраические структуры итерационных функций
 в системах защиты информации» по специальности
 05.13.19 – Методы и системы защиты информации, информационная безопасность
 на соискание ученой степени доктора физико-математических наук

Наименование организации, дата и номер приказа о назначении научным консультантом	Приказ по научно-учебному комплексу «Информатика и системы управления» МГТУ им. Н.Э. Баумана от 04.07.2013 № 03.02–02/18
Фамилия, имя, отчество	Погорелов Борис Александрович
Гражданство	Гражданин Российской Федерации
Ученая степень (с указанием шифра и наименования научной специальности и отрасли науки, по которым защищена диссертация)	Доктор физико-математических наук, 20.03.04 (информация о наименовании специальности закрыта)
Ученое звание (по какой кафедре / по какой специальности)	Профессор по специальной кафедре
Академическое звание	Действительный член Академии криптографии Российской Федерации
Почетное звание	Заслуженный деятель науки Российской Федерации
Основное место работы	Информация о месте работы и занимаемой должности закрыта
Список основных публикаций научного консультанта по теме диссертации в рецензируемых научных изданиях за последние 5 лет (не более 15 публикаций)	
1.	Погорелов Б. А. Факторструктуры преобразований / Б. А. Погорелов, М. А. Пудовкина // Математические вопросы криптографии. – 2012. – Т. 3, вып. 3. – С. 81–104.
2.	Погорелов Б. А. Комбинаторная характеристика XL-слоев / Б. А. Погорелов, М. А. Пудовкина // Математические вопросы криптографии.– 2013. – Т. 4, вып. 3. – С. 99–129.
3.	Погорелов Б. А. О расстояниях от подстановок до импримитивных групп при фиксированной системе импримитивности / Б. А. Погорелов, М. А. Пудовкина // Дискретная математика. – 2013. – Т. 25, вып. 3. – С. 78–95. <i>в переводной версии журнала:</i> Pogorelov B. A. On the distance from permutations to imprimitive groups for a fixed system of imprimitivity / B. A. Pogorelov, M. A. Pudovkina // Discrete Mathematics and Applications. – 2014. – Vol. 24, is. 2. – P. 95–108. – DOI: 10.4213/dm1249
4.	Погорелов Б. А. Орбитальные производные над кольцом вычетов. Часть I. Общие свойства / Б. А. Погорелов, М. А. Пудовкина // Математические вопросы криптографии.– 2014. – Т. 5, вып. 4. – С. 99–127.
5.	Погорелов Б. А. О расстояниях от подстановок до объединения всех импримитивных групп с равными параметрами систем импримитивности / Б. А. Погорелов, М. А. Пудовкина // Дискретная математика. – 2014. – Т. 26, вып. 1. – С. 103–117. <i>в переводной версии журнала:</i> Pogorelov B. A. On the distance from permutations to the union of all imprimitive groups with identical parameters of imprimitivity systems / B. A. Pogorelov, M. A. Pudovkina // Discrete Mathematics and Applications. – 2014. – Vol. 24, is. 3. – P. 163–173. – DOI: 10.4213/dm1271

6.	Погорелов Б. А. Надгруппы аддитивных регулярных групп порядка 2^n кольца вычетов и векторного пространства / Б. А. Погорелов, М. А. Пудовкина // Дискретная математика. – 2015. – Т. 27, вып. 3. – С. 74–94. – DOI: 10.4213/dm1336
7.	Погорелов Б. А. Орбитальные производные по подгруппам и их комбинаторно-групповые свойства / Б. А. Погорелов, М. А. Пудовкина // Дискретная математика. – 2015. – Т. 27, вып. 4. – С. 94–119. – DOI: 10.4213/dm1350
8.	Погорелов Б. А. Орбитальные производные над кольцом вычетов. Часть II. Вероятностно-комбинаторные свойства / Б. А. Погорелов, М. А. Пудовкина // Математические вопросы криптографии. – 2015. – Т. 6, вып. 1. – С. 117–133.
9.	Burov D. A. An attack on 66 rounds of Khazad / D. A. Burov, В. А. Pogorelov // Математические вопросы криптографии. – 2016. – Т. 7, вып. 2. – С. 35–46.
Прочие публикации научного консультанта по теме диссертации за последние 5 лет	
10.	Погорелов Б. А. О приближении подстановок импримитивными группами / Б. А. Погорелов, М. А. Пудовкина // Прикладная дискретная математика. Приложение. – 2011. – № 4. – С. 17–18.
11.	Погорелов Б. А. О комбинаторных свойствах группы, порождённой XL-слоями / Б. А. Погорелов, М. А. Пудовкина // Прикладная дискретная математика. Приложение. – 2012. – № 5. – С. 22–23.
12.	Погорелов Б. А. $\otimes_{w, ch}$ -марковские преобразования / Б. А. Погорелов, М. А. Пудовкина // Прикладная дискретная математика. Приложение. – 2015. – № 8. – С. 17–19.
13.	Погорелов Б. А. Свойства группы, порождённой группами сдвигов векторного пространства и кольца вычетов / Б. А. Погорелов, М. А. Пудовкина // Прикладная дискретная математика. Приложение. – 2015. – № 8. – С. 15–16.
14.	Погорелов Б. А. О группах, порождённых преобразованиями смешанного типа и группами наложения ключа/ Б. А. Погорелов, М. А. Пудовкина // Прикладная дискретная математика. Приложение. – 2016. – №. 9.– С. 14–16.

Научный консультант

Б. А. Погорелов

Сведения подтверждаются по месту назначения научным консультантом.

Верно

Руководитель научно-учебного комплекса
«Информатика и системы управления»,
заведующий кафедрой «Информационная безопасность»,
Заслуженный деятель науки Российской Федерации,
доктор технических наук,
профессор



В. А. Матвеев

27.06 . 2016 г.