Сведения об официальном оппоненте
по диссертации **Черепнева Михаила Алексеевича**
«О вычислительной сложности алгоритмов факторизации и дискретного логарифмирования» по специальности 01.01.09 – дискретная математика и математическая кибернетика.

Фамилия, имя, отчество	Фролов Александр Борисович
Ученая степень и наименование отрасли науки	Доктор технических наук
Научная специальность, по которой оппонентом защищена диссертация	05.13.01-Системный анализ, управление и обработка информации
Полное наименование организации в соответствии с уставом	Федеральное государственное бюджетное образовательное учреждение высшего образования «Национальный исследоватнльский университет «МЭИ»
Сокращённое наименование организации в соответствии с уставом	ФГБОУ ВО НИУ МЭИ
Ведомственная принадлежность	Министерство образования и науки Российской Федерации
Место нахождения	г. Москва
Почтовый индекс, адрес организации	111250, г. Москва, ул. Красноказарменная, д. 14
Структурное подразделение	Кафедра математического моделирования
Должность оппонента	профессор
Телефон	8-915-1772687
Адрес электронной почты	abfrolov@mail.ru
Список публикаций по теме диссертации соискателя в рецензируемых научных изданиях за последние 5 лет (не менее 5 и не более 15 публикаций)	1. Гашков С.Б., Фролов А.Б. Сравнительный анализ вычислений с использованием сочетанийразличных базисов конечных полей. Вестник МЭИ. 2017. №1. С. 58-66. 2. Гашков С.Б., Фролов А.Б., Лукин С.А. Оптимальные нормальные базисы 2-го и 3-го типов вполях характеристики семь. Вестник МЭИ. 2016. №1. С. 44-49. 3. Фролов А.Б. Понижение границы неустойчивости неинтерактивных протоколовидентификации. Вестник МЭИ. №1, 2015. С. 114-120. 4. Затей А.В., Фролов А.Б. Схемы предварительного распределения ключей с хешированием,допускающие коалиции. ВестникМЭИ. №6 , 2013, с. 166-172. 5. Sergey Gashkov, Alexander Frolov, Igor Sergeev. Arithmetic in Finite Fields Supporting Type-2 or Type-3 Optimal Normal Bases. Advances in Intelligent Systems and Computing Volume 470 2016 Dependability Engineering and Complex Systems

	Proceedings of the Eleventh International Conference on Dependability and Complex Systems DepCoS-RELCOMEX. June 27–July 1, 2016, Brunow, Poland Springer International Publishing. 2016. PP. 157-168 Author ID: 9277433600 Scopus 6. SergeyGashkov, AlexanderFrolov, SergeyLukin, OlgaSukhanva/ ArithmeticintheFinitefieldsUsing Optimal Normal and Polynomial Bases in Combination. In Advances in Intelligent Systemsand Computing. V. 365. Theory and Engineering of Complex Systems and Dependability.Proceedings of the Tenth International Conference on Dependability and Complex SystemsDepCos-RELCOMEX, June 29-july 3 2015. P. 153-162. Номер IDS: BD9QU Идентификационныйномер: WOS:000365127100015 Author ID: 9277433600 Web of Science 7. Alexander Frolov, Alexander Vinnikov. FSM Simulation of Cryptographic Protocols UsingAlgebraic Pr0cessor. In Proceedings of the Ninth International Conference on Dependability andComplex systems DepCoS-RELCOMEX, June 30-Juy 4,2014. P.189-198. Номер IDS: BD8BGИдентификационныйномер: WOS:000363748100018 Author ID: 9277433600WebofScience 8. Alexander Frolov. Improving of Non-Interactive Zero-Knowledge Arguments Using ObliviousTransfer\New Results in Dependability and Computer Systems (Book Title).Advances inIntelligent Systems and Computing (Series Title) Volume 224, Springer-Verlag, Berlin,Heidelberg. 2013. 153-171. Номер IDS: BD8BF Идентификационныйномер:WOS:000363745900014 AuthorID: 9277433600 WebofScience

Официальный оппонент Фролов А.Б.
« 17 » апреля 2017 года

Подпись и сведения заверяю

М.П.

Заместитель начальника
Управления по работе с персоналом
Л.И.Полевая