

## ОТЗЫВ

на автореферат диссертационной работы Пудовкиной Марины Александровны «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации», представленной на соискание учёной степени доктора физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Информационная безопасность является одной из важнейших сфер национальной безопасности Российской Федерации и её значение только возрастает. Применение средств обеспечения информационной безопасности зарубежного производства содержит в себе значительные угрозы для России и ее граждан особенно в области информационно-коммуникационных технологий и при использовании возможностей, предоставляемых глобальной информационной сетью Интернет. Подтверждением этому, в частности, являются разоблачения экс-сотрудника ЦРУ Эдварда Сноудена.

Не неся ничего фундаментально нового для технических специалистов-экспертов в сфере информационной безопасности, разоблачения Сноуденом программ спецслужб США подтвердили, что кибершпионаж, киберагрессия и незаконный сбор персональных данных в локальных и глобальных информационных сетях несут стратегическое преимущество для государств, которые практикуют такие методы, и в то же время стратегическую угрозу безопасности и интересам стран и их граждан – объектов такой деятельности.

При этом государство – агрессор (в данном случае США) контролирует и использует в своих целях производство, распространение и применение средств защиты информации, которые, рекламируются фирмами-производителями, как «эффективные средства» защиты от угроз и опасностей, исходящих, в том числе, со стороны тех же спецслужб США. В этом плане, в документах, опубликованных с подачи Сноудена, описаны гигантские масштабы сотрудничества между Кремниевой долиной и спецслужбами США.

Так, ради безудержной и не всегда законной наживы, ведущие компании США, такие как Microsoft, Google, Yahoo, Facebook, YouTube, Skype, AOL, Apple, PalTalk и др., охотно идут на указанное сотрудничество, обманывая при этом потребителей (отличных от спецслужб США) своей продукцией в международном масштабе. Например, Microsoft для привлечения внимания пользователей к своим программным продуктам, затеял маркетинговую кампанию, стартовавшую в апреле 2013 года, под девизом «Ваша конфиденциальность важна для нас». Но в то же самое время, как указывает Сноуден, эта интернет-компания предоставляла АНБ возможность обходить собственную криптографическую защиту для того, чтобы получить доступ к письмам и чатам портала Outlook.com. Кроме того, сотрудникам американских спецслужб был представлен прямой доступ к облачному хранилищу файлов сервиса SkyDrive, имеющего более 250 миллионов пользователей по всему миру.

Таким образом, разработка и создание доверенных отечественных технологий и средств защиты информации, отвечающих российским стандартам и требованиям информационной безопасности, относится к первоочередному направлению обеспечения национальной безопасности России. Судя по автореферату, на разработку теоретического обеспечения определенного направления в решении этой актуальной задачи нацелены исследования, проведённые в диссертационной работе Пудовкиной Марины Александровны.

В отечественной науке защиты информации, выдающимся представителем и одним из главных создателей которой является научный консультант соискателя, действительный член Академии криптографии РФ, д.ф.-м.н., профессор Погорелов Б.А., большое внимание при разработке технологий и средств защиты информации уделяется алгебраическим методам. В русле этого направления находится и диссертационная работа М.А. Пудовкиной. Она посвящена исследованию комбинаторных и

алгебраических структур итерационных функций в системах защиты информации.

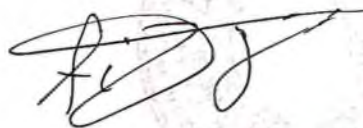
Судя по тексту автореферата, все результаты диссертации изложены на строгом математическом языке, обладают внутренним единством и являются новыми. Использованный в диссертации математический аппарат относится к алгебре и дискретной математике. Следует отметить максимальную общность постановок задач и их решения.

Существенных недостатков автореферата диссертации обнаружить не удалось. Можно отметить отдельные стилистические погрешности (например, на стр. 4).

Результаты диссертации могут быть применены для обеспечения выполнения необходимых требований при разработке отечественных средств защиты информации.

Вывод: судя по автореферату, диссертация Пудовкиной Марины Александровны соответствует требованиям, предъявляемым к докторским диссертациям, и её автор заслуживает присуждения учёной степени доктора физико-математических наук.

Доктор физико-математических наук  
(специальность 20.03.04,  
информация о наименовании специальности закрыта)  
ведущий советник Главного управления развития  
информационных и телекоммуникационных технологий  
Министерства обороны Российской Федерации



Алиев Физули Камирович

29.03.2017 г.

Адрес: 119160, г. Москва, Фрунзенская наб., д. 22/2.

Главное управление развития информационных и телекоммуникационных технологий Министерства обороны Российской Федерации