

## ПАМЯТИ УЧИТЕЛЯ

К величайшему сожалению, 16 декабря 2020 г. ушёл из жизни Геннадий Петрович Агибалов — основатель и бессменный главный редактор журнала «Прикладная дискретная математика».



Геннадий Петрович Агибалов родился 17 мая 1939 г. в селе Казанцево Шушенского района Красноярского края. В 1961 г. окончил радиофизический факультет Томского государственного университета (ТГУ) и до конца жизни работал на педагогических и научных должностях в ТГУ, заведовал кафедрами электронной вычислительной техники и автоматики, математической логики и проектирования, лабораторией синтеза дискретных автоматов.

В 1968 г. он защитил кандидатскую диссертацию на тему криптографической защиты управляющей информации, в 1993 г. — докторскую, посвящённую теории дискретных автоматов на полурешётках.

С 1972 г. Г. П. Агibalов возглавлял в ТГУ ведущую научную школу прикладной дискретной математики, известную в мире созданными в ней русским языком программирования и автоматизированными системами логического проектирования, достижениями в криптографии, теории автоматов, компьютерной безопасности. На базе этих достижений он создал в ТГУ кафедру защиты информации и криптографии (в 1999 г.) и лабораторию компьютерной криптографии (в 2018 г.).

В 2002 г. Г. П. Агibalов организовал Всероссийскую конференцию «Сибирская научная школа-семинар с международным участием “Компьютерная безопасность и криптография” — SIBECRYPT», которая с тех пор с неизменным успехом каждый год проходит в разных городах и весях Сибири, собирая до 60 участников из многих городов Российской Федерации, а также Белоруссии и Украины.

В 2008 г. Г. П. Агibalов основал ежеквартальный журнал «Прикладная дискретная математика». До конца жизни он был его главным редактором, через его руки проходили все статьи, которые он внимательно прочитывал, правил (а зачастую и полностью переписывал) английские аннотации. Под руководством Геннадия Петровича журнал вошёл в перечень ВАК, международные базы цитирования Scopus, WoS, MathSciNet и Zentralblatt MATH.

Образовательная программа ТГУ по специальности «Компьютерная безопасность», разработанная Г. П. Агibalовым, трижды (2011–2013 гг.) по оценкам независимого органа — журнала «Аккредитация в образовании» — входила в число лучших образовательных программ инновационной России.

В 2015 г. Государственная Дума Российской Федерации присвоила кафедре защиты информации и криптографии звание «Образовательный центр года РФ в области информационной безопасности»; её студенты Олег Брославский (2015 г.) и Артём Ивачёв (2016 г.) получили звание «Студент года РФ в области информационной безопасности».

Студенческая команда SiBeags кафедры — трёхкратный чемпион России и многократный призёр международных соревнований CTF в области информационной безопасности.

Г. П. Агibalов награждён нагрудными знаками «Почётный работник высшего профессионального образования Российской Федерации» (2003 г.) и «Почётный работник науки и техники Российской Федерации» (2009 г.).

По результатам научной деятельности в области прикладной дискретной математики и криптографии Г. П. Агibalов опубликовал более 100 статей в рецензируемых журналах и сборниках, 5 монографий и 4 учебных пособия. Под его руководством успешно защищены 12 кандидатских и 3 докторских диссертации.

Наиболее крупным научным достижением Г. П. Агibalова является создание им в 1980-х — начале 1990-х гг. основ теории дискретных автоматов на полурешётках, открывших новое научное направление на стыке алгебры (полурешёток), дискретной математики (дискретных функций и автоматов) и математической кибернетики (управляющих систем), в рамках которого, помимо решения некоторых чисто алгебраических задач, относящихся к кодированию полурешёток и полурешёточно упорядоченным алгебрам, ему впервые удалось формализовать такие понятия, относящиеся к дискретным автоматам, как динамическое поведение (вызываемое асинхронным изменением входных сигналов), его физическая реализуемость, адекватная модель и её точность, и все традиционные задачи логического проектирования, включая задачи эквивалентных преобразований, минимизации, декомпозиции, кодирования, моделирования, анализа, синтеза, функциональной полноты и др., решить в постановке, отражающей динамику поведения автомата, возможность её физической реализации на

современной электронной базе и адекватность моделирования с любой наперед заданной точностью. Докторская диссертация Г. П. Агибалова на эту тему признана в ВАК РФ лучшей за 1993 г. по специальности 05.13.01.

Последние 20 лет научной деятельности Г. П. Агибалова были целиком посвящены непосредственно криптографии и её применениям в компьютерной безопасности. В ряду результатов исследований, проведённых им в этот период, можно отметить: алгоритмы криптоанализа некоторых симметричных и асимметричных шифров (2000 г.); метод линеаризационного множества в решении систем уравнений над конечным полем и линеаризационная атака на генераторы ключевого потока (ГКП) со сложностью меньше, чем у корреляционной атаки (2003 г.); алгоритмы криптоанализа сжимающего и самосжимающего ГКП методом решения их систем логических уравнений (2004 г.); вероятностные схемы симметричного поточного шифрования над конечным полем со свойством совершенности (2005 г.); элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом и алгоритм такого криптоанализа методом решения системы уравнений последнего раунда (2008 г.); элементы теории статистических аналогов дискретных функций и их применение в криптоанализе итеративных блочных шифров с эффектом более высоким, чем у линейного криптоанализа М. Matsui (2010 г.); описание криптосистем с функциональными ключами на базе векторных булевых функций и конечных автоматов (2014 г.); условия обратимости с конечной задержкой конечных автоматов для различных типов обратимости (2017 г.).

Геннадий Петрович был очень увлечённым человеком, всегда полон идей — будь то новое понятие, необходимое для решения научной проблемы, или ещё одно спортивное состязание в честь Дня кафедры (в которых, к слову, сам Геннадий Петрович неизменно участвовал), или неожиданное (порой экзотическое) место проведения школы-семинара SIBECRYPT ... Он заражал своим энтузиазмом всех вокруг, не боялся трудностей (коих было немало), никогда не делал выбор в пользу чего-то, что было бы выгодно ему лично, но «неправильно» в целом или вредило бы его Делу.

Геннадий Петрович Агибалов навсегда останется в сердцах и душах коллег и учеников, и мы все, бесконечно скорбя о невозможной потере, будем всё же осознавать своё счастье от того, что нам довелось встретиться с таким Человеком, учиться у него и работать рядом с ним.

О своём отношении к жизни, Родине, работе, людям лучше всего сказал сам Геннадий Петрович в своём стихотверении.

От имени коллег и учеников  
И. А. Панкратова

## МЫ

(штрихи к автопортрету)

Все поколения в жизни проходили  
Стихии, войны, мор иль гнет властей,  
И только мы сторонкой проскочили  
От этих самых гибельных страстей.

Нам повезло, мы начали с Победы,  
Которую отцы нам принесли,  
И 50 спокойных лет безбедно  
Учились и трудились, как могли.

Трудились не за деньги, не за славу  
И не искали сверхпостов себе;  
Желали одного — чтоб за державу  
Не стыдно было нам в своей судьбе.

Ценили честь превыше, чем карьеру,  
И поступали, совесть как вела,  
Свободными в достаточную меру  
Мы оставались в мыслях и делах.

Не верили ни в Бога и ни в Чёрта,  
Но свято чтили славный красный флаг,  
И никогда под членов в «Волгах» чёрных  
Не прогибались ради личных благ.

Мы оставляли близких без вниманья,  
Нам было некогда согреть родных.  
Любили мать с отцом на расстояньи,  
О, как теперь нам не хватает их!

Друзей нередко всею обижали,  
Но их обиды вмиг прощали им,  
Учителей посмертно вспоминали,  
Но забывали позвонить живым.

Политика нас слабо занимала,  
Прохвосты ж находились всякий раз,  
И вот однажды всей страны не стало  
И вместе с нею отменили нас.

Теперь цивилизованные страны,  
Спасённые Россией от врагов,  
Как те монголы, требуют с нас дани,  
А мы не в силах вразумить их вновь.

Есть дети, внуки и работы много,  
Но на душе великая тоска:  
Бессмысленная жизнь, и у порога  
Уже стоит надгробная доска.

Одна лишь просьба к поколениям новым:  
Когда наш луч сверкнёт из вечной тьмы,  
Вы нас хорошим помяните словом —  
Не самые плохие были мы.

*Г. П. Агибалов*  
23.02.2001