ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ

13 июля 1970 г. приказом Министерства высшего и среднего специального образования РСФСР в составе Томского университета был создан факультет прикладной математики. В начале 80-х гг. он был переименован в факультет прикладной математики и кибернетики.

Структура факультета

Кафедра исследования операций (зав. – проф. А.М. Горцев). Открыта в 1978 г.

Кафедра прикладной математики (зав. – проф. Ю.И. Параев). Открыта в 1970 г.

Кафедра теоретической кибернетики (зав. – проф. Ю.Г. Дмитриев). Открыта в 1970 г.

Кафедра теории вероятностей и математической статистики (зав. – проф. А.А. Назаров). Открыта в 1974 г.

Кафедра высшей математики и математического моделирования (зав. – проф. В.В. Конев). Открыта в 1970 г.

Кафедра программирования (зав. – проф. А.Ю. Матросова). Открыта в 1970 г.

Кафедра защиты информации и криптографии (зав. – проф. Г.П. Агибалов). Открыта в 1999 г.

Вычислительный центр (нач. – Б.И. Савинков). Открыт в 1985 г.

Направления и специальности: «прикладная математики и информатика» (010500), «математические методы в экономике» (080116), «компьютерная безопасность» (090102).

Научные направления, развиваемые коллективом преподавателей факультета, и основные полученные результаты посвящены глобальным проблемам кибернетики: оптимизация извлечения, переработки и использования информации.

Кадровый состав: 57 преподавателей, их них 18 профессоров, докторов наук, 31 доцент, кандидат наук, в аспирантуре обучается 39 человек.

Декан факультета – проф. А.М. Горцев.

7 апреля 2009 г. кафедра защиты информации и криптографии отметила свое 10-летие. Приказ ректора об открытии новой кафедры на ФПМК вышел 7 апреля 1999 г. Тогда это событие воспринималось как одно из рядовых организационных мероприятий, коих в жизни ТГУ случалось и ещё будет случаться немало. Надо обеспечить учебный процесс по новой специальности – вот и создали новую кафедру. Вот именно: не новорождённая, а новая! Иная, значит. Не такая, как все. «С лица не общим выраженьем». И не инновационная. Скорее – классическая в классическом университете, т.е. то «новое, что есть хорошо забытое старое», когда по-прежнему научные исследования и сотрудники кафедры определяют содержание и уровень подготовки специалистов на кафедре. Отсюда вытекает и всё остальное, а именно:

– кафедра ежегодно проводит Международную конференцию под названием «Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» – SibeCrypt», на которую съезжаются до 100 учёных, аспирантов и студентов из научных учреждений и университетов Москвы, Санкт Петербурга, Саратова, Екатеринбурга, Омска, Новосибирска, Томска, Красноярска, Иркутска и других городов России, а также Украины, Беларуси.

– кафедра ежеквартально издает всероссийский научный журнал «Прикладная дискретная математика» – «ПДМ», в котором публикуются статьи отечественных и зарубежных авторов по всем важнейшим разделам дискретной математики (дискретные функции и автоматы, целые числа, алгебраические системы, коды, графы и т.п.) и её приложениям в криптографии, компьютерной безопасности, информатике и программировании, логическом проектировании, интеллектуальных системах, в синтезе надёжных вычислительных и управляющих систем и др. и который рекомендован УМО Минобрнауки РФ в области информационной безопасности всем вузам страны для использования в научных исследованиях и учебном процессе в этой области;

– ежегодно до 10 студентов кафедры принимают участие с научными докладами, иногда и пленарными, в Международной конференции SibeCrypt и публикуют свои научные статьи в журнале «ПДМ», делая то и другое, как правило, без соавторства в лице преподавателей кафедры и проходя рецензирование на равных с маститыми учёными;

– на базе кафедры создана и получает подготовку молодёжная команда ТГУ SiBears, участвующая регулярно в международных соревнованиях CTF (Capture The Flag) по защите компьютерной информации и занимающая в них призовые места среди трёх-четырёх десятков команд университетов мира (в 2009 г. она стала чемпионом России и завоевала 2-е место на чемпионате мира);

– студенты кафедры становятся победителями и призёрами студенческих олимпиад по математике, информатике, базам данных, английскому языку и философии от университетского до республиканского уровней, им присуждаются Потанинские, вузовские и правительственные стипендии, их дипломные работы признаются среди лучших на всероссийских конкурсах студенческих научных работ (в 2009 г. – работа Александра Панина), они выходят в УМНИКи (в 2009 г. – Наталья Кушик и Дмитрий Стефанцов);

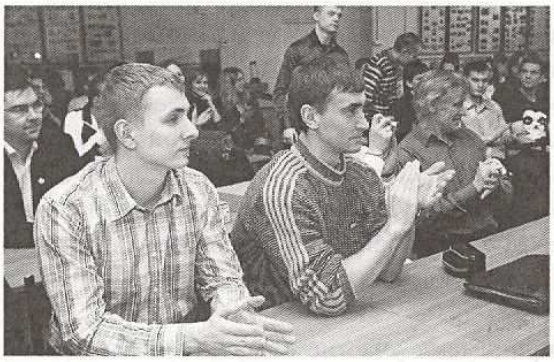
– учебный процесс, прикладные научные исследования и издательскую деятельность кафедра осуществляет на основе свободного программного обеспечения, развивая в студентах, как в старое доброе время, умение создавать, исследовать и развивать собственные программные продукты и избавляя их от необходимости тупого использования готового и не контролируемого ими лицензионного программного обеспечения, к тому же ещё и дорогостоящего;

– при кафедре открыта бесплатная школа юного криптографа, в которой под руководством ведущих преподавателей кафедры учащиеся 8–11-х классов школ города знакомятся с историей криптографии, её ролью в истории человечества, с необходимыми элементами дискретной математики, разбирают и решают различные криптографические задачи с целью профориентации и подготовки к участию в российских олимпиадах по математике и криптографии;

– с 2008 г. кафедра ежегодно организует и проводит в ТГУ Всероссийскую межрегиональную олимпиаду по математике и криптографии для школьников Томска, в 2009 г. её дипломами отмечены и два юных криптографа кафедры (Михаил Котов и Никита Небаев);

– значимой частью жизни кафедры являются праздничные мероприятия, проводимые ею ежегодно по случаю своего дня рождения, в которых участвуют почти все преподаватели и студенты кафедры (а это более 100 человек) и многие её выпускники прошлых лет, которые все вместе и каждый в отдельности на радость себе и другим демонстрируют свои способности, знания, волю, характер в многочисленных баталиях на футбольном поле и волейбольной площадке, за шахматной доской и в математической олимпиаде, на научной конференции и в конкурсах тематических тортов и стенгазет и в апофеозе всего – в концертной программе с атрибутами весёлого студенческого капустника, сопровождаемого всеобщим товарищеским чаепитием;

– на кафедре стало традицией проводить 1 сентября «чай первокурсника» и 13 февраля «чай выпускника» – дни, в которые в семейной обстановке за чашкой чая работники кафедры, соответственно, знакомятся лично с каждым из «новобранцев» и прощаются с каждым из своих очередных выпускников, даря им памятные презенты и говоря одним



Юбилей кафедры защиты информации

приветственные, а другим напутственные слова с пожеланиями всех благ и удачи в учёбе – одним и в работе и в личной жизни – другим;

– кафедра имеет свои символы – гимн, вальс, клятву, логотип, значок, в которых отражен сам дух кафедры: профессиональная направленность, высокая нравственность, преданность Родине, любовь к людям, непрерывные совершенствование и труд.

Кто-то может сказать, что всё это мелочи; главное – качество образования, объём грантов и внебюджетных средств, рейтинг по системе показателей и т.п. Действительно, качество образования – это, безусловно, самое главное в работе любой кафедры. Вчитайтесь ещё раз в перечисленные выше «мелочи» и убедитесь, что все они направлены именно на повышение качества обучения, да ещё – на улучшение воспитания, без которого специалистов «двойного применения», каковых готовит кафедра, и выпускать-то нельзя. А о том, какого качества специалисты выпускаются кафедрой, можно судить, например, по следующему факту: все 15 её выпускников 2009 г. защитили дипломные работы на «отлично», 9 из них получили «красные дипломы», в том числе 6 – «абсолютно красные», т.е. без единой оценки меньше 5 за 5 с половиной лет обучения, и все 15 пошли работать по персональным заявкам от предприятий.

Наконец, юбилейный год кафедры ознаменовался ключевым для неё событием: Денис Колегов стал первым её выпускником, получившим учёную степень кандидата наук. В этом событии особенно примечателен тот факт, что учёная степень присуждена ему за научные результаты, достигнутые именно по полученной на кафедре специальности – компьютерной безопасности.

Что касается оценки кафедры по количеству зарабатываемых ею денег, рейтингу и прочему, то, по большому счёту, такая оценка от лукавого, но и здесь кафедра не последняя: в 2009 г. она получила грант РФФИ размером 192 тыс. руб. на проведение школы-семинара SibeCrypt, грант ФЦП «Кадры» размером 500 тыс. руб. на проведение Международной конференции «Компьютерная безопасность и криптография» с элементами научной школы для молодёжи и грант ФЦП «Кадры» размером 2,5 млн руб. на выполнение научно-исследовательского проекта «Разработка и исследование технологии и инструментальной среды создания защищённых систем обработки информации» и успешно освоила эти средства.

Согласитесь, с неплохими показателями подошла кафедра к своему первому 10-летию.

50 лет научной школе прикладной дискретной математики

2009 г. был годом 50-летия ведущей научной школы прикладной дискретной математики ТГУ (далее: Школа). Её рождение мы относим к 1959 г. Именно тогда в Докладах Академии наук СССР (Т. 129, № 4, С.729–731) вышла в свет первая научная статья аспиранта РФФ Аркадия Дмитриевича Закревского «Метод синтеза функционально-устойчивых автоматов», послужившая истоком для развития в ТГУ нового научного направления, изначально связанного с созданием и применениями электронных вычислительных машин (ЭВМ) и в разные периоды становления Школы называвшегося разными терминами, отражавшими наиболее значимые достижения Школы в эти периоды, – теорией релейных схем, цифровой автоматикой, технической логикой, теорией дискретных автоматов, логическим проектированием, автоматизацией синтеза, автоматизацией решения логико-комбинаторных задач и, наконец, прикладной дискретной математикой. Последнее название Школы и её научного направления наиболее полно отражает современный уровень развития научных исследо-

ваний в Школе, охватывающих практически все области приложения и компьютеризации современной дискретной математики – дискретные функции и автоматы, логические и автоматные уравнения, компьютерную алгебру, вычислительные методы в теории чисел, математическую и компьютерную криптографию, надёжность вычислительных и управляющих систем, интеллектуальные системы, компьютерную безопасность, информатику и программирование, параллельные комбинаторные алгоритмы и многое другое.

В своём развитии Школа не оставалась всегда цельным коллективом, что вполне естественно. Сначала (во второй половине 1960-х гг.) из Школы вышла группа из 6 исследователей, обосновавшихся в Севастополе, в том числе те «четверо под одной крышей» – Е.А. Бутаков, В.В. Кирюхин, В.Г. Новосёлов и В.И. Островский, которые, в бытность студентами, за свою коллективную дипломную работу по автоматизации синтеза цифровых автоматов под руководством А.Д. Закревского в 1961 г., едва ли не первыми в ТГУ, получили Золотую медаль АН СССР. В самом начале 1970-х гг. сам А.Д. Закревский и 7 других его учеников переехали в Минск, где в АН Беларуси до сих пор продолжают исследования, начатые в Школе, поддерживая с нею научные и добрые человеческие отношения.

А.Д. Закревский среди участников IV Сибирской научной школы-семинара SIBECRYPT'05

С отъездом А.Д. Закревского бремя сохранения Школы легло, как это часто бывает в подобных случаях, на его наиболее «поперечного» ученика – автора этих строк, оказавшегося, говоря без ложной скромности, и наиболее преданным своему учителю. (К сожалению, не всегда такое бывает). Эта преданность, а также понимание значимости Школы для университета, в том числе и некоторыми его влиятельными руководителями, в частности тогдашним директором СФТИ М.А. Криовым, спасли Школу от поглощения её «интеллектуальной и материальной собственности» другими научными коллективами, позволили ей войти в ряд ведущих научных школ ТГУ, известных своими достижениями не только в нашей стране, но и за рубежом.

Воистину выдающимся научно-техническим достижением Школы прикладной дис-кретной математики ТГУ является «русский язык программирования», как в своё время американские учёные назвали язык программирования ЛЯПАС, разработанный в Школе в 1960-х гг. под руководством А.Д. Закревского и реализованный на всех отечественных и ряде зарубежных (в Польше, США, ФРГ) ЭВМ, включая современные персональные компьютеры. Язык предназначен для представления алгоритмов решения задач именно дискретной математики и по своим операционным возможностям для этого значительно превосходит все другие языки программирования общего пользования, в том числе и созданные много позже. В 1970–1980-е гг. на предприятиях министерств электронной и радиопромышленности СССР с большим экономическим эффектом применялись системы автоматического синтеза и диагностики дискретных автоматов, созданные в Школе на базе ЛЯПАСа.

Алгоритмический язык ЛЯПАС и системы автоматизации программирования на нём, предвосхитившие многие идеи, воплощённые широко, эффектно, но, отнюдь, далеко не эффективно, в современных забугорных языках программирования и операционных системах, – это, вне всякого сомнения, явление мирового уровня, безусловная гордость не только Школы и ТГУ, но и всей российской науки на все времена.

Особое и очень важное место в Школе всегда занимали и занимают криптографические исследования, связанные с защитой информации и компьютерной безопасностью. Впервые автор этих строк прочитал научную работу по криптографии ещё в 1960 г., будучи студентом 4-го курса университета. Это была рукопись А.Д. Закревского, посвящённая

применению конечных автоматов для шифрования с закрытым ключом. К сожалению, А.Д. Закревский не принадлежит к числу тех, кому в ту пору было позволено заниматься криптографией, и его рукопись никогда не была опубликована под тем предлогом, высказанным «чёрным» рецензентом, что её результаты «совершенно секретны». Для восстановления исторической справедливости мы впервые, спустя 50 лет после написания, опубликовали её в журнале «Прикладная дискретная математика» № 2 за 2009 г. В ней в качестве шифратора предложен конечный автомат с функцией выходов, биективной в каждом состоянии. Ныне такие автоматы хорошо изучены под названием шифрующих, ввиду чего рукопись уже не имеет прежней научной ценности, но она чрезвычайно интересна с методической и исторической точек зрения. Она написана так просто и увлекательно, что её, несмотря на некоторые несовременные криптографические термины в ней, можно и нужно смело рекомендовать всякому начинающему криптографу. Мы опубликовали рукопись в её первозданном виде, без каких-либо купюр и редакторской правки, чтобы не исказить её первоначального духа, который один захватит любого читателя, в том числе и искушённого в криптографии. Мы опубликовали её, сохраняя полностью терминологию того времени и авторский стиль изложения, совершенно безупречный с методической точки зрения. Наконец, мы опубликовали её как реликвию, если не всей российской криптографии, то уж по меньшей мере научной Школы прикладной дискретной математики ТГУ.

В 50-летней истории криптографии в Школе можно выделить 3 периода, назвав их условно военным, переходным и гражданским.

В первый период (1960-е гг.) исследования по криптографии в Школе проводились по заказу оборонного предприятия и носили закрытый характер. Они велись, что называется, «с чистого листа», в отсутствие какой-либо литературы по этому предмету, опираясь в основном на собственные представления задач криптографии и волю заказчика. В значительной степени это были наивные исследования, но в их процессе было уяснено главное: создание стойких криптосистем, говоря современным языком, невозможно без их тщательного криптоанализа. Именно алгоритмы криптоанализа некоторых поточных шифров и полученные с их помощью оценки стойкости последних и стали основными достижениями наших исследований этого периода. Именно таким путём мы доказали тогда непригодность линейных автономных автоматов в качестве генераторов ключевого потока, обескуражив тем самым учёных из МВТУ им. Н.Э. Баумана, предложивших такие генераторы нашему заказчику. Некоторые результаты тех наших исследований, в частности, относящиеся к генераторам нормальных рекуррентных последовательностей и к автоматным генераторам ключевого потока с функцией выхода в качестве ключа, до сих пор не превзойдены и по-прежнему актуальны.

На исходе этого периода в Школе был проявлен интерес и к теории кодирования как к средству для создания кодовых систем шифрования. Впервые в мировой науке мы разработали пакет программ (на языке ЛЯПАС) для решения алгоритмических задач теории кодирования, но так случилось, что наши исследования кодовых шифрсистем были отложены на целых 30 лет. К сожалению, по человеческому простодушию вашего покорного слуги, в отношения нас с заказчиком вмешался генерал Козлов, и заказчику было запрещено прибегать к нашим криптографическим услугам. Через 40 лет история повторится, но это будет уже в другой стране, с другим заказчиком и при другом генерале.

Второй период развития криптографии в Школе (1970–1980-е гг.) был периодом осмысления полученных результатов, их легализации и обобщения в рамках теории экспериментов с автоматами и приобщения к ним студентов. С позиций чистой криптографии это был «вялотекущий» период, идущий в отсутствие заказчика и стимулов с его стороны, но в этот период нами была разработана применяемая и ныне технология решения комбинаторно-логических задач, каковыми, собственно и являются задачи анализа и синтеза криптоалгоритмов, а также была развита теория декомпозиции конечных автоматов – одного из инструментов создания современных конечно-автоматных криптосистем с открытым ключом. Монография Школы 1985 г. на эту тему остаётся до сих пор единственной отечественной книгой по декомпозиции автоматов.

Третий период развития криптографии в Школе (с 1990-х гг.) связан с известными переменами в стране и с появлением возможности проведения открытых теоретических и экспериментальных исследований в этой области. Нельзя сказать, что в теоретическом плане наши исследования этого периода значительно более глубокие, чем прежние, но они охватывают практически всю проблематику современной «гражданской криптографии».

В настоящее время Школа представлена тремя кафедрами – защиты информации и криптографии (на ФПМК), программирования (на ФПМК) и информационных технологий в исследовании дискретных структур (на РФФ) и готовит специалистов по трём специальностям: «компьютерная безопасность», «прикладная математика и информатика», «радиофизика и электроника». В советское время Школа имела ещё и базовую научно-исследовательскую лабораторию в СФТИ, насчитывавшую до 30 штатных единиц научных сотрудников. Именно лаборатория служила фундаментом, на котором стояла Школа как единый научный коллектив. В новой стране, где место науки заняла инноватика, этого фундамента у Школы, как и у страны, к сожалению, не стало, и она, как и страна, переживает, мягко говоря, не лучшие свои времена. Но времена приходят и уходят, а Школа остаётся в её учениках.

Г.П. Агибалов,
заведующий кафедрой защиты информации
и криптографии ФПМК