ТЕХНОСФЕРА

Уважение к минувшему – вот черта,
отделяющая образованность от дикости.
А.С. Пушкин

СОЗИДАТЕЛИ ОТЕЧЕСТВЕННОЙ ЭЛЕКТРОНИКИ

**Серия книг-сборников,
каждая из которых посвящена
одному из видных деятелей,
коллективу или направлению
отечественной электроники**

Серия основана Б.М. Малашевичем в 2010 г.

УДК 082.2 + 519.6
ББК 94 + 22.19
М18

СОЗИДАТЕЛИ ОТЕЧЕСТВЕННОЙ ЭЛЕКТРОНИКИ
Выпуск 5
Вильжан Мавлютинович Амербаев

Автор-составитель и редактор Малашевич Б.М.
М.: ТЕХНОСФЕРА, 2021. – 572 с., более 200 илл.
ISBN 978-5-94836-609-8

Настоящая книга продолжает серию книг-сборников «Созидатели отечественной электроники» (серия СОЭ).

Пятый сборник серии СОЭ посвящён видному советскому, российскому и казахстанскому математику, доктору технических наук, профессору, академику Национальной АН Республики Казахстан, лауреату Государственной премии СССР Вильжану Мавлютиновичу Амербаеву, выдающемуся специалисту в областях вычислительной техники: вычислительной математики, модулярной арифметики, цифровой обработки изображений и сигналов, криптологии, алгебраического кодирования и других методов цифровой обработки информации.

УДК 082.2 + 519.6
ББК 94 + 22.19

ISBN 978-5-94836-609-8

СОЗИДАТЕЛИ ОТЕЧЕСТВЕННОЙ ЭЛЕКТРОНИКИ

Выпуск 5

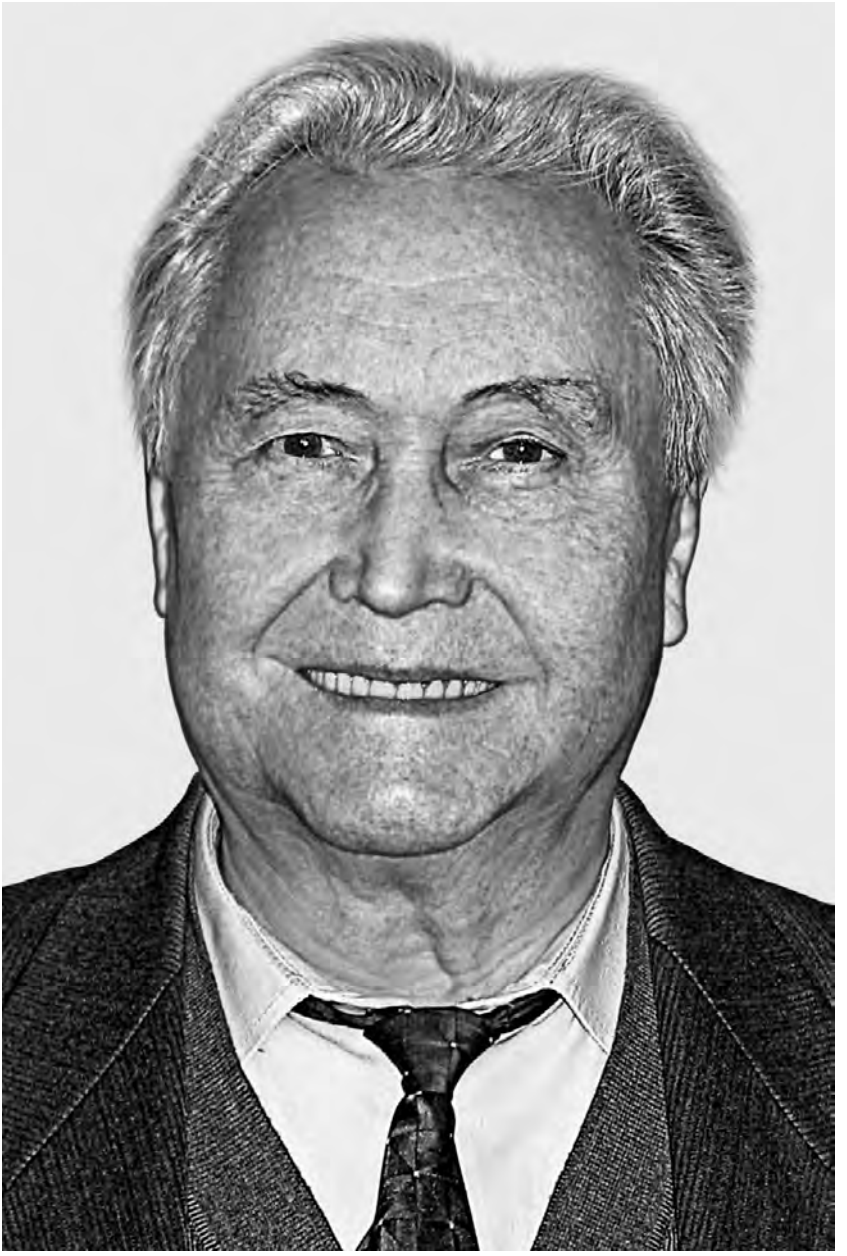
Вильжан Мавлютинович Амербаев

научный редактор
акад. А.Л. Стемпковский

Техносфера
Москва
2021

Я понял,
насколько мудра, мила и доброжелательна
математика,
а также её носители и просветители.
Я на всю жизнь остался верен ей.
Служба ей приносила мне плоды радости труда
и мироощущения.
Мне и сейчас не чужды эти ощущения.
Я прекрасно понимаю, что математика – это океан
и что я освоил лишь крохотный кусочек берега
этого океана.
Но и этого хватило на всю жизнь,
чтобы наслаждаться океаном на этом берегу.

В. Амербаев
в беседе с аспирантами



Вильжан Мавлютинович Амербаев

Из патентов В.М. Амербаева

Содержание

Из монографий В.М. Амербаева

ВВЕДЕНИЕ

Вильжан Мавлютинович Амербаев – учёный-новатор в вычислительной математике

Вильжан Мавлютинович Амербаев – выдающийся специалист в области компьютерной алгебры, параллельных вычислений, теории арифметического кодирования информации, цифровой обработки сигналов и операционного исчисления.

Научную деятельность Вильжан Мавлютинович начал ещё будучи студентом физико-математического факультета Казахского государственного университета им. С. М. Кирова (КазГУ) в г. Алма-Ате – столице Казахской ССР, который окончил в 1954 г. с красным дипломом.

В 1963 г., работая в должности заведующего лабораторией машинной и вычислительной математики АН КазССР, он защитил диссертацию кандидата физико-математических наук на тему «*Численные методы обращения интегрального преобразования Лапласа*» в Математическом институте им. В. А. Стеклова АН СССР (МИАН) в Москве.

С тех пор вычислительная математика стала основным профессиональным делом его жизни.

В 1965 г. В. М. Амербаев заинтересовался новым тогда направлением вычислительной математики — непозиционной системой счисления остаточных классов (СОК) и продемонстрировал оригинальный подход к её развитию. В результате он был приглашён на работу в Москву в НИИ физических проблем зеленоградского Центра микроэлектроники, где тогда разрабатывался конкурсный эскизный проект модулярной (на основе СОК) супер-ЭВМ «Алмаз» для полигонной системы противоракетной обороны (ПРО) «Аргунь».

Здесь он вместе с вверенным ему небольшим коллективом разработал вариант модулярной арифметики, обеспечивший высочайшее для тех времён быстродействие ЭВМ в 30 млн оп/с (типовое тогда быстродействие ЭВМ — 300 тыс. оп/с).

В результате проект «Алмаз» выиграл конкурс у проектов главных конструкторов Лебедева С. А. (ИТМиВТ) и Карцева М. А. (ИНЭУМ), а Центр микроэлектроники получил заказ на разработку технического проекта ЭВМ 5Э53 с быстродействием в 40 млн оп/с (главный конструктор Юдицкий Д. И.).

Для получения такого быстродействия В. М. Амербаевым был разработан вариант двухступенчатой непозиционной модулярной арифметики. А для перспективного проекта ЭВМ IV поколения им была разработана принципиально новая табличная модулярная арифметика, в которой результаты не вычислялись, а считывались из ПЗУ (в связи с малой разрядностью оснований СОК это уже тогда было практически реализуемо).

Результаты работ В. М. Амербаева в этот период нашли отражение в многочисленных публикациях и монографиях, а также в его докторской диссертации на тему «*Вычисления в кольце главных идеалов и их приложения в вычислительной технике*», которую он защитил в 1971 г. на учёном совете зеленоградского НИИ микроприборов.

В 1972 г. В. М. Амербаев был приглашён в Алма-Ату на должность заместителя директора по научной работе Института математики и механики АН КазССР, в создании которого он ранее принимал активное участие. Здесь им была создана алмаатинская научная школа математиков, проводящая серьёзные фундаментальные исследования в области вычислительной (в т. ч. модулярной) математики и в её применении при решении важнейших в республике прикладных задач.

В том же 1972 г. В. М. Амербаев был избран членом-корреспондентом АН КазССР.

В 1977 г. В. М. Амербаев по медицинским показаниям был вынужден покинуть высокогорную Алма-Ату (800 м над уровнем моря) и вернуться в равнинный Зеленоград, в котором к этому времени в результате крупной реорганизации все работы по высокопроизводительным многоразрядным ЭВМ (а значит, и по модулярной арифметике, не эффективной в малоразрядных мини- и микро-ЭВМ) были прекращены. В этот период Вильжан Мавлютинович работал в вузах, сначала в МИИГА,

затем в МИЭТ, где преподавательскую работу совмещал с научными исследованиями и подготовкой аспирантов.

В 1988 г. В. М. Амербаева пригласили в АН КазССР, где он был избран действительным членом АН, членом президиума АН КазССР и академиком-секретарём отделения физико-математических наук.

В 1991 г. Вильжан Мавлютинович в группе видных учёных России, Белоруссии, Украины и Казахстана был удостоен звания лауреата Государственной премии СССР по науке и технике «*за разработку и внедрение в народное хозяйство систем измерения позиционно-модулярного типа*».

Огромную работу по организации физико-математических наук Казахстана Вильжан Мавлютинович сочетал с научными исследованиями и подготовкой аспирантов и докторантов. В частности, он был инициатором и руководителем междисциплинарной программы «Динамический хаос в распределённых системах», проводил исследования проблемы универсальности генетического кода, предложив модулярную арифметику в качестве эффективного инструмента исследований. Под его руководством разработана концепция развития информатики в Казахстане, информатизации республики и многое другое. Исследования в модулярной арифметике привели его к разработке новой концепции построения интромодулярных вычислительных систем, развитой им впоследствии в Зеленограде.

В 1994 г. В. М. Амербаев возвращается в Зеленоград, в МИЭТ, где он сочетает преподавательскую работу с научными исследованиями по развитию модулярной арифметики, её применению в криптографии, в алгоритмах шифрования в целях повышения скорости криптографического преобразования путём распараллеливания процедур арифметических операций.

В 2004 году В. М. Амербаев был приглашён на работу в Институт проблем проектирования в микроэлектронике (ИППМ) РАН, где и проработал последние весьма плодотворные годы своей жизни. В ИППМ РАН он возглавил созданную для него новую лабораторию эффективных методов вычислений. Следует отметить, что его работы в ИППМ РАН с привлечением группы молодых учёных привели к появлению новых результатов:

модулярной логарифметики, рекурсивной модулярной арифметики и др.

Результаты научной деятельности В. М. Амербаева отражены в более 210 его научных трудах, в т. ч. в 13 монографиях. Основные научные публикации относятся к областям теории кодирования, параллельных вычислений, помехоустойчивого арифметического кодирования, численных методов обращения интегральных преобразований Лапласа, свёрточных уравнений.

Светлая память о Вильжане Мавлютиновиче Амербаеве, выдающемся учёном и прекрасном человеке, навсегда сохранится в сердцах его близких, друзей, коллег, учеников, всех его знавших.

Основоположники отечественной модулярной арифметики:
Акушский И. Я., Юдицкий Д. И., Амербаев В. М., 1960-е годы

ГЛАВА I

ТВОРЧЕСКИЙ ПУТЬ ВИЛЬЖАНА МАВЛЮТИНОВИЧА АМЕРБАЕВА

Вильжан Мавлютинович Амербаев

Вильжан Мавлютинович Амербаев — доктор технических наук, профессор вычислительной математики, академик Национальной академии наук Республики Казахстан (ранее АН КазССР), лауреат Государственной премии СССР по науке и технике (1991 г.).

Выдающийся математик СССР, России и Казахстана, специализировавшийся в областях компьютерной алгебры, вычислительной математики, теории арифметического кодирования информации, распараллеливания вычислений, модулярной арифметики и логарифметики, цифровой обработки сигналов, криптозащиты информации, операционного исчисления, численных методов обращения интегральных преобразований Лапласа, сверхточных уравнений...

Сочетал фундаментальные исследования новых направлений вычислительной математики с практической реализацией их результатов при построении реальных систем обработки информации. Его фундаментальные исследования и практические разработки были направлены на повышение эффективности вычислительной техники: производительности, надёжности, точности, защищённости информации.

Вильжаном Мавлютиновичем создана широко известная в стране и за рубежом школа вычислительной математики, результатом работы многочисленных учеников которой стали более 210 научных трудов на русском, английском и корейском языках (в т. ч. 13 монографий).

Научная деятельность Вильжана Мавлютиновича происходила в структурах АН КазССР (ныне Национальная академия наук Республики Казахстан (НАН РК)) и зеленоградского Центра микроэлектроники СССР и РФ. Поэтому описание его научного пути мы представляем двумя соответствующими статьями.

Здание АН КазССР (НАН РК) на фоне гор Заилийского Алатау, в котором работал академик-секретарь В. М. Амербаев

Научно-организационная деятельность академика НАН РК Вильжана Мавлютиновича Амербаева

Пак И. Т., д. т. н., профессор, академик РАЕН, заслуженный деятель науки и техники РК

Иван Тимофеевич Пак

Вильжан Мавлютинович Амербаев был профессиональным математиком — воспитанником Казахского государственного университета имени С. М. Кирова и Математического института имени В. А. Стеклова АН СССР. Его творческий путь начался ещё со студенческой скамьи, когда он участвовал в научных семинарах со своими научными докладами, выполненными под руководством академика К. П. Персидского. Затем в течение двух лет, работая в качестве ассистента кафедры дифференциальных уравнений КазГУ, продолжал исследования в области устойчивости дифференциальных уравнений, начатые в студенческие годы. Но ему пришлось сменить научное направление.

В то время в Казахстане начало зарождаться новое научное направление, связанное с применением вычислительной техники и вычислительной математики в различных областях народного хозяйства и в научных исследованиях. В республике не было ни одного специалиста с учёной степенью, поэтому остро стоял вопрос о подготовке таких специалистов в этой области. И Амербаев В. М., как наиболее подготовленный, в 1956 г. был направлен в аспирантуру лаборатории машинной и вычислительной математики (ЛМВМ) АН КазССР

Константин Петрович Персидский

по специальности «вычислительная математика» с прикомандированием к научному руководителю В. А. Диткину в вычислительный центр АН СССР.

В аспирантуре Вильжану Мавлютиновичу, прежде чем приступить к исследованиям по теме диссертации, пришлось самым серьёзным образом готовиться к сдаче кандидатского минимума, поскольку он быстро понял, что, к сожалению, полученные знания в КазГУ были весьма поверхностными. И он был вынужден с головой окунуться в учёбу и практически заново изучать математику.

Дело в том, что кандидатский экзамен в аспирантуре принимали не формально, как было принято в вузах Алма-Аты. Вопросы кандидатского экзамена носили творческий характер. Экзаменуемый должен был не только формально доказать теорему, но и привести решения при различных изменениях условий теоремы. Имея поверхностные и формальные знания предмета, невозможно было этого сделать. Рассказывая об этом, Вильжан Мавлютинович признавался, что только в вычислительном центре и Математическом институте им. В. А. Стеклова он по-настоящему понял суть математики. И только с этого момента для Вильжана Мавлютиновича математика стала настоящей профессией. За три года пребывания в аспирантуре Вильжан Мавлютинович не успел подготовить диссертацию, так как почти два года из трёх он по-настоящему познавал математику. Пришлось ему после окончания срока аспирантуры ещё три года, будучи зачисленным на работу младшим научным сотрудником в лабораторию машинной и вычислительной математики, быть прикомандированным в вычислительный центр Академии наук СССР. Только в 1963 году ему удалось подготовить и защитить в Математическом институте

На ноябрьской демонстрации, 1962 г. Амербаев В. М. (второй справа) с сотрудниками Академии наук КазССР

На ноябрьской демонстрации, 1964 г. Амербаев В. М. (первый слева) с сотрудниками ЛМВМ

им. В. А. Стеклова диссертацию на тему «Некоторые численные методы обращения интегрального преобразования Лапласа». Диссертационная работа Вильжана Мавлютиновича посвящена разработке методов восстановления оригинала путём разложения его в ряд по ортогональным многочленам на конечном промежутке.

Лаборатория машинной и вычислительной математики

К 1962 году лаборатория машинной и вычислительной математики, которая была создана в 1954 году при президиуме АН КазССР, оказалась без руководителя. В лаборатории не было ни одного остепенённого человека, и единственный, кто мог бы быть на этой должности, — это Вильжан Мавлютинович.

Постановлением президиума Академии наук КазССР за подписью президента Академии наук К. И. Сатпаева Вильжан Мавлютинович становится заведующим лабораторией. Лаборатория, являясь самостоятельной структурой при президиуме академии наук, не имела в своём штате хозяйственной группы. А дел общехозяйственных и организационных в лаборатории оказалось много. Одной из основных задач лаборатории было обеспечение научных исследований вычислительной техникой и необходимыми программными средствами. В то время это было неординарной задачей.

В условиях острого дефицита специалистов необходимо было организовать бесперебойную работу первой в Казахстане ЭВМ «Урал-1». Она работала с большими перебоями, в основном из-за плохого обеспечения отвода тепла, выделяемого тысячей электронных ламп. К тому же отсутствовали квалифицированные специалисты-электронщики по обслуживанию ЭВМ. На инженерные должности вынуждены были брать выпускников физического факультета КазГУ и «автоматчиков» политехнического института. В Казахстане и даже в Союзе только начали подготовку специалистов по эксплуатации ЭВМ. Эти трудности вкупе с отсутствием специальных помещений для машины создавали колоссальные проблемы по обеспечению вычислительными ресурсами научных исследований.

Лаборатория машинной и вычислительной математики не имела своего постоянного помещения, перебрасывалась из одного места в другое. Вот пример: ЭВМ «Урал-1» с трудом установлена в только что выстроенном здании гостиницы ВДНХ. Не успели как следует обустроить помещение для монтажа ЭВМ, как тут же потребовалось освободить его для использования по назначению. В конце концов все-таки пришлось освободить помещение, а «Урал-1» передать физико-математической школе. А для сотрудников выделили место на территории физических

На демонстрации 1-го мая, 1973 г.
Слева Амербаев В. М., Аяпберегенов Б., Пак И. Т., Амандосов А.

институтов, расположенных в пос. Алатау, в 25 км от здания Академии наук КазССР. Сотрудники добирались на работу и обратно в город специальным 20-местным автобусом и автомобилем ГАЗ-69.

Для лаборатории надо было приобрести новую вычислительную технику. Уже давно появились в стране ЭВМ второго поколения на базе полупроводников, а лаборатория была оснащена устаревшими настольными клавишными машинами, аналоговой ЭВМ ИПТ-5 и электронным вычислителем ЭВ-80, выполняющим только 32 стандартные команды, задаваемые путём жёсткой коммутации на коммутационной доске.

Тем не менее на этой скудной вычислительной технике выполнялись НИР по тематике «Теория и практика механизации и вычислений» и осуществлялись следующие работы (перечислены только главные):

- механизация подсчётов запасов полезных ископаемых Качарского месторождения магнетитовых железных руд (результаты работ были переданы в Министерство геологии и охраны недр КазССР и получили одобрение);
- решение задачи циклонного энергометаллургического процесса, предусматривающее разработку программы для решения на электронной счётной машине уравнений циклонного процесса плавки. Программа представляла из себя нормальную систему из пяти дифференциальных уравнений, содержащую 22 различных параметра, которые оказывают влияние на общее движение горящих частиц. Разработанная программа решения этой задачи была передана в Институт энергетики для использования в исследованиях процессов плавки в циклонных камерах;
- таблицы тропосферной составляющей зодиакального света для Астрофизического института АН КазССР;
- вычислительные работы для Института ядерной физики АН КазССР, связанные с исследованиями вылета высокоэнергичных тяжёлых осколков при нуклон-ядерных взаимодействиях;

- вычисление интенсивности флуоресцентного излучения выхода вторичного излучения с учётом взаимного влияния компонентов для Института металлургии и обогащения АН КазССР;
- статистическая обработка данных о больных силикозом на свинцовых рудниках для Института краевой патологии АН КазССР.

Все эти работы проводились при непосредственном руководстве Вильжана Мавлютиновича Амербаева.

С приобретением новой ЭВМ связана целая история. Для начала необходимость её покупки надо было аргументированно обосновать у себя в президиуме АН КазССР. Затем после получения разрешения у нас эта процедура повторилась в Центракадемснабе АН СССР. Финансирование для новой ЭВМ было добыто у себя в республике. С этими делами Вильжан Мавлютинович справился успешно. В результате заявка на ЭВМ второго поколения — БЭСМ-3М была принята с решением выделить её в 1966 году. Надо было подготовиться к приёму ЭВМ, а готовых площадей не было, но ему все-таки удалось получить разрешение занять помещение столовой в здании президиума АН КазССР, которая переехала в новое, выстроенное для неё здание.

Институт математики и механики

Параллельно Вильжан Мавлютинович активно участвовал в подготовке создания Института математики и механики. Ему вместе с академиками К. П. Персидским, О. А. Жаутыковым, членом-корреспондентом Е. И. Кимом удалось определить научное направление создаваемого института, которое было утверждено отделением математики Академии наук СССР. Ему не раз приходилось ездить в Москву к корифеям науки Н. Н. Боголюбову (академику-секретарю отделения математики АН СССР) и И. М. Виноградову, директору Математического института имени В. А. Стеклова, отстаивать и доказывать необходимость создания института. Удалось ему обосновать

и направление по вычислительной математике и вычислительной технике.

Открытие Института математики и механики состоялось в сентябре 1965 года на базе сектора математики и механики и лаборатории машинной и вычислительной математики. В новом институте Вильжан Мавлютинович проработал всего четыре месяца.

Модулярная арифметика

В то время в зеленоградском Научном центре микроэлектроники было начато проектирование ЭВМ высокой производительности на базе нетрадиционной так называемой модулярной арифметики. Израиль Яковлевич Акушский, основатель лаборатории машинной и вычислительной математики в Казахстане, приехал в Алма-Ату со своим директором — талантливым инженером, главным конструктором проектируемой модулярной ЭВМ 5Э53 Давлетом Исламовичем Юдицким.

На их семинарах Вильжан Мавлютинович «загорелся» новым направлением в машинной арифметике. Прирождённый талант математика позволил ему сразу «разглядеть» перспективность модулярной арифметики. А приезжие гости увидели в нем квалифицированного умного математика, которого как раз искали. Было сделано предложение, которое было принято Вильжаном Мавлютиновичем. В начале 1966 года он уехал в Москву, но связь с Алма-Атой поддерживал постоянно. Я часто пользовался его советами, поскольку проводимые им исследования по вопросам вычислительной техники и вычислительной математики пришлось принять мне.

В 1971 году В. М. Амербаев защитил докторскую диссертацию на тему «Вычисления в кольце главных идеалов и их приложения в вычислительной технике». В ней разработаны алгебраическая концепция параллельных вычислений, принципы арифметического самокорректирующего кодирования. Частные реализации этой концепции легли в основу проектирования арифметического процессора высокопроизводительной вычислительной системы 5Э53.

В машинном зале ЭВМ «Минск-32», 1973 г.
В первом ряду слева направо: Амербаев В. М., Пак И. Т., Пильщиков Е.

Заместитель директора Института математики и механики

К началу 1970-х годов в Институте математики и механики все ещё не было ни одного специалиста по вычислительной математике и вычислительной технике с докторской степенью, а институт остро нуждался в таком специалисте. Вильжан Мавлютинович уже был доктором наук. На президиуме Академии наук КазССР было предложено вернуть его. И в 1971 году он был приглашён в Алма-Ату на должность заместителя директора Института математики и механики. Уже в следующем 1972 году Вильжан Мавлютинович избирается членом-корреспондентом АН КазССР. Первым директором Института математики и механики был известный казахстанский математик, подготовивший десятки кандидатов наук, Константин Петрович Персидский. В 1970 году он по собственному желанию

ушел с поста директора, и директором стал академик Асан Дапсович Тайманов, но он вскоре тоже ушёл, а его место занял ученик академика Сергея Михайловича Никольского Тулебай Идрисович Аманов. К моменту приглашения Вильжана Мавлютиновича Амербаева в институт микроклимат в коллективе оставлял желать лучшего. А с приходом Вильжана Мавлютиновича ситуация стала постепенно выправляться. Отношения между отделами математики, механики, вычислительной математики и вычислительной техники улучшились. Заработали регулярные научные семинары в каждом отделе. Возвращение Вильжана Мавлютиновича сыграло важную роль в развитии вычислительной математики в Казахстане. Кроме того, получило толчок важное направление создания различных информационных систем, а также теория кодирования.

Под руководством Вильжана Мавлютиновича разработана концепция развития информатики в Казахстане, в которой основной упор делался на увлечённость этим направлением

На конференции, посвящённой 40-летию Института математики и механики, 2005 г. В первом ряду слева направо: Жаутыков О. А., Никольский С. М., Амербаев В. М.

молодых кадров. В Казахском государственном университете организованы новые кафедры по информатике. ЭВМ БЭСМ-3М эксплуатировалась круглосуточно, для интенсификации исследований удалось обосновать заказ на приобретение более совершенной ЭВМ «Минск-32». Будучи заместителем директора, он с головой окунулся в улучшение и активизацию научно-организационной работы в институте, в первую очередь по мобилизации научных сил и привлечению молодых специалистов к выполнению приоритетных для Казахстана научно-исследовательских работ. В этот период открываются новые лаборатории: теории кодирования, методов оптимизации, больших систем, комбинаторных методов теории информации.

Молодые учёные тянулись к нему, а он щедро делился своими знаниями. С 1971 по 1976 гг. во время работы Вильжана Мавлютиновича в институте становятся кандидатами наук Лян Э. Н., Устинов В. А., Амангельдиев Б. Р., Шигаев М., Утебаев Н. Г., В. И. Полывянный. Будучи членом академии наук, он с академиками О. А. Жаутыковым, Н. С. Ержановым, Ж. С. Такибаевым и членом-корреспондентом Е. И. Кимом, представляя отделение физико-математических наук, принимал участие в разработке стратегии развития физико-математических наук в Казахстане.

В тот период Казахстан испытывал острый недостаток в специалистах высокой квалификации — кандидатах и докторах наук. Являясь членом объединённого диссертационного совета по защите кандидатских диссертаций по математике и физике, Вильжан Мавлютинович оказывал всяческое содействие многим молодым талантливым математикам в получении кандидатских степеней. Кроме того, Вильжан Мавлютинович всегда находил время для активного участия в пропаганде физико-математических знаний среди школьников и привлечения их через малую академию наук (академия наук для школьников) к научно-исследовательской работе через проведение различных научных конкурсов.

Вильжан Мавлютинович очень серьёзно и мудро относился к поддержке перспективных молодых людей. Вспоминается такой эпизод. В начале 1970-х годов в институте математики

появились очень сильные ребята — выпускники центральных вузов, среди них был талантливый молодой человек, выпускник Московского государственного университета, ученик известного математика Бориса Моисеевича Левитана. Прибыл он в институт, будучи уже кандидатом наук. Но со своей «колокольни», воспитанный в духе математиков МГУ, увидел, что институтские научные семинары проводятся на недостаточно высоком научном уровне, а в журналах печатаются и слабые статьи. Он стал высказывать критические замечания публично — на семинарах и в кулуарах института. Конечно, его опрометчивость и нетактичность объяснялись чрезмерным задором и жизненной неопытностью молодого человека. Но это сильно отразилось на его научной карьере. Талантливый математик с учёной степенью кандидата наук, он долго не мог подняться выше должности младшего научного сотрудника. Вильжан Мавлютинович, видя его математические способности, своим авторитетом учёного и организатора науки смог добиться избрания молодого учёного старшим научным сотрудником. Этим молодым человеком был ныне известный академик, лауреат премии Казахстана по науке Отелбаев Мухтарбай Отелбаевич. Ему уже за 70 лет, он возглавляет Астанинский филиал Московского государственного университета.

Приведу ещё один пример. В Астрофизическом институте работал выпускник Ленинградского университета, астрофизик по базовой специальности. Природа наградила его талантом учёного с прекрасными математическими знаниями, но у него не было учёной степени. Он неординарно мыслил, намного превосходил своих коллег по теоретической подготовке. И, как многие одарённые люди, молодой человек имел непростой характер. В институте, где он работал, руководство и ведущие учёные плохо понимали и воспринимали его идеи. Вильжан Мавлютинович, будучи академиком — секретарём отделения физико-математических наук, организовал при отделении городской междисциплинарный семинар под названием «Открытые системы», где принимали участие молодые учёные из институтов астрофизики, ионосферы, физико-технического и Казахского государственного университета. Активным участником этих семинаров

был вышеупомянутый талантливый астрофизик, Николай Григорьевич Макаренко. Вильжан Мавлютинович заметил его, стал всячески поддерживать, в скором времени рекомендовал на работу в Институт математики и механики (тогда он уже назывался Институтом теоретической и прикладной математики) младшим научным сотрудником. Хотя Н. Г. Макаренко не имел учёных степеней, но по уровню знаний, научным результатам и публикациям соответствовал даже учёной степени доктора наук. С его приходом в институте стало развиваться новое прикладное направление — компьютерное моделирование. Вокруг него организовалась группа около десяти молодых специалистов, впоследствии ставших кандидатами наук. В их числе и сам Н. Г. Макаренко, который долго отказывался готовить материал для защиты вначале кандидатской (1995 г.), а затем докторской диссертации (2005 г.). В настоящее время Н. Г. Макаренко вместе со мной работает в Институте информационных и вычислительных технологий, успешно проводит исследования в области обработки цифровых сигналов для распознавания образов, финансируемые грантами Минобрнауки РК. Как крупный специалист в этой области, Н. Г. Макаренко широко востребован: он принимает участие в работах Государственной астрофизической обсерватории и Назарбаев Университета.

Таких примеров, когда Вильжан Мавлютинович всячески поддерживал перспективных молодых людей, много, некоторые из них сами расскажут об этом в своих воспоминаниях в данной книге.

Вильжан Мавлютинович, отдавая много сил и времени научно-организационной работе, всегда оставался профессиональным математиком. Он успешно проводил исследования и в области криптографии. Его работы по использованию модулярной арифметики в алгоритмах шифрования в целях повышения скорости криптографического преобразования путём распараллеливания процедур арифметических операций в вычислительных системах привели к разработке новой концепции построения интромодулярных вычислительных систем. Эта концепция базируется на принципе глубокого распараллеливания процедур модульных вычислений модулярной

арифметики. Интромодулярные вычисления открывают пути эффективной реализации парадигмы гомоморфных облачных вычислений на однородной вычислительной среде с гибким управлением надёжностью вычислений в целом. Им также было введено понятие левообратимой бинарной операции, которое было использовано при создании блочных шифров, что позволяет существенно повысить скорость процедур шифрования, ориентированных на параллельную и конвейерную обработку данных. С учетом бурного роста потребностей в повышении скоростей передачи и обработки данных такая задача представляется востребованной. В то же время такие способы шифрования должны обеспечивать высокие криптографические, инженерно-криптографические и специальные свойства блочных шифров.

Разработка способов шифрования с возможностью их параллельной и конвейерной организации является объективной потребностью на современном этапе развития техники. Эти возможности являются несомненным преимуществом предложенной структуры. На описанный способ криптографического преобразования был получен патент.

В 1976 году по семейным обстоятельствам Вильжан Мавлютинович вынужден был оставить институт и возвратиться в Москву, передав руководство отделом вычислительной математики и вычислительной техники мне. Перед отъездом президент Академии наук КазССР Аскар Минлиахмедович Кунаев предложил Вильжану Мавлютиновичу должность главного учёного секретаря президиума Академии наук. В. М. Амербаев обещал подумать, но президент по неизвестной нам причине изменил свое решение. Вильжан Мавлютинович вернулся к работе в зеленоградском Научном центре и одновременно стал заведующим кафедрой математики московского Института гражданской авиации.

Учёный, педагог и организатор науки в независимом Казахстане

В 1986 году произошли декабрьские события в Казахстане (выступление молодёжи на площади Республики по поводу

назначения из центра в качестве первого секретаря ЦК КП Казахстана Г. В. Колбина вместо Д. А. Кунаева). В Союзе начались демократические преобразования. После серьёзной критики в адрес президента Академии наук КазССР А. М. Кунаева (родной брат Первого секретаря ЦК Компартии Казахстана) А. М. Кунаев был освобождён от занимаемой должности. Президентом Академии КазССР был избран лауреат Ленинской премии биолог Мурат Абенович Айтхожин. Новый президент пригласил на пост одного из вице-президентов академика Умирзака Махмутовича Султангазина, в то время работавшего главным учёным секретарём президиума АН КазССР. К сожалению, М. А. Айтхожин, проработав не более двух лет, ушёл из жизни (1987). И по рекомендации ЦК Компартии Казахстана президентом впервые в истории Академии наук Казахстана стал математик, академик У. М. Султангазин — ученик известного академика Г. И. Марчука, тогда президента Академии наук СССР. У. М. Султангазин после окончания КазГУ работал там же до 1978 года, пройдя путь от ассистента до заведующего кафедрой. В том же году после смерти директора института математики Тулебая Идрисовича Аманова он был назначен на должность директора Института математики и механики.

У. М. Султангазину уже в качестве президента АН КазССР необходимо было набрать команду управленцев. Это было непростое время — в Союзе под влиянием демократических сил происходили большие изменения во всех сферах деятельности. Выборы депутатов, первых руководителей разного калибра проходят на альтернативной основе. Спокойная жизнь в стране уже позади. Обстоятельства времени требовали коренным образом изменить и деятельность академии наук, которая изначально и всегда была самостоятельной и самодостаточной организацией, объединяющей в своём составе ведущих учёных в виде действительных членов — академиков и членов-корреспондентов. И главное, академия наук состояла из научно-исследовательских институтов различных отраслей науки — физико-математических, наук о земле, биологических, химико-технологических, общественных...

К началу 1990-х годов отделение физико-математических наук состояло из пяти институтов: математики и механики, ядерной физики, физики высоких энергий, ионосферы, астрофизики. В 1991 г. президент АН КазССР У. М. Султангазин добивается перед директивными органами открытия ряда новых научно-исследовательских институтов. В отделении физико-математических наук происходят коренные изменения. И здесь приглашённый президентом У. М. Султангазиным в качестве академика-секретаря отделения физико-математических наук Вильжан Мавлютинович Амербаев принимает самое активное участие в реструктуризации институтов и их научных направлений.

В этом месте хочу сделать небольшое отступление от своего основного текста: У. М. Султангазин, став президентом академии наук, не в пример другим руководителям добровольно отказался от должности директора Института математики и механики, руководя которым в течение 10 лет, он добился больших успехов. У. М. Султангазин вывел отсталый, постоянно занимавший последние места в социалистических соревнованиях институт на призовые места. Институт был удостоен переходящего Красного знамени Совета министров СССР. Директором института после Султангазина в результате выборов на альтернативной основе стал член-корреспондент АН КазССР, ученик известного академика А. В. Бицадзе Назарбай Кадырович Блиев. Он сумел сохранить традиции как в направлении научных исследований, так и в демократичности административного управления. В институте образца 1991 года работало около 400 человек в составе трёх крупных отделов математики, механики, кибернетики. По решению президиума АН КазССР на базе Института математики и механики было создано пять самостоятельных институтов: Институт теоретической и прикладной математики (директор Н. К. Блиев), Институт механики (директор У. М. Джолдасбеков), Институт проблем информатики и управления (директор А. А. Ашимов), Институт космических исследований (директор академик У. М. Султангазин), Институт прикладной математики в Караганде (директор Е. С. Смаилов). Институт физики высоких энергий отделения физико-математических наук был

реорганизован и разделён на два института — физико-технический (директор Б. Н. Мукашев) и физики высоких энергий (директор Э. Г. Босс). В этих преобразованиях и определении научных направлений новых институтов существенная роль принадлежит академику-секретарю отделения Вильжану Мавлютиновичу Амербаеву.

В 1994 году в связи с уходом У. М. Султангазина с поста президента В. М. Амербаев снова уезжает в Москву.

Остановлюсь ещё на одной заслуге Вильжана Мавлютиновича. Казахстан испытывал недостаток в высококвалифицированных кадрах по группе специальностей информатики. Основной причиной было отсутствие специализированных диссертационных советов по защите кандидатских и докторских диссертаций, а их открытие было затруднено из-за отсутствия докторов наук по этим специальностям. Решение было найдено Вильжаном Мавлютиновичем после переговоров с представителями — докторами наук по специальности «алгебра и теория чисел». Таким образом, в 1991 году впервые в Казахстане под его председательством создаётся специализированный диссертационный совет по защите докторов и кандидатов наук по двум специальностям: «вычислительные машины, системы и сети» и «алгебра и теория чисел». Впоследствии после отъезда Вильжана Мавлютиновича совет возглавлял Ваш покорный слуга. Далее по мере появления новых докторов наук появилась возможность создать совет по группе специальностей информатики («вычислительные машины, системы и сети» и «математическое моделирование и численные методы») уже без специальности «алгебра и теория чисел». Совет существовал до конца принятия новой формы подготовки кадров высшей квалификации, т. е. до 2010 года. Совет сыграл огромную роль в подготовке казахстанских докторов и кандидатов наук, которые работают во многих научно-исследовательских учреждениях и вузах Казахстана.

Вильжан Мавлютинович был не только большим талантливым учёным, профессионально ориентирующимся во всех областях математической науки, но и прекрасным педагогом, свободно и доходчиво доносящим свои знания, мысли, идеи

многочисленным ученикам. В его докладных записках, различных письмах времён его служебной деятельности в Академии наук КазССР всегда прослеживалась чёткая, убедительная логика.

Основные направления научной деятельности и монографии

Основные его научные исследования относятся к областям компьютерной алгебры и цифровых методов обработки сигналов, теории кодирования, параллельных вычислений, помехоустойчивого арифметического кодирования, численных методов интегральных преобразований Лапласа, сверхточных вычислений и криптографии. Результаты отражены в более чем 200 печатных научных работах и заявках на изобретения. Он является автором ряда обстоятельных и актуальных монографий. Многие из рассматриваемых в них вопросов впервые поднимаются в научной литературе, в т. ч. в монографиях.

1. «Основы машинной арифметики комплексных чисел»

В 1970 г., в период его работы в Москве (1966–1971), тиражом 800 экз. вышла монография, являющаяся продолжением моей кандидатской диссертации, под названием «Основы машинной арифметики комплексных чисел» (авторы В. М. Амербаев, И. Я. Акушский, И. Т. Пак). В монографии было затронуто важное направление машинной арифметики — обобщение системы остаточных классов на объекты более сложной природы, чем область вещественных чисел. Эта работа начиналась в Институте математики и механики под руководством Вильжана Мавлютиновича Амербаева. Построение системы счисления, следующей в области комплексных чисел, оказалось возможным на основе гауссовой теории целых комплексных чисел. Гауссова идея изоморфизма между комплексными вычетами числа по комплексному модулю и его вещественными вычетами по норме этого модуля создала возможность работать в вещественной области в целом без разбиения комплексного числа на вещественное и мнимое. В первых трёх главах представлены основные вопросы теории делимости, теории сравнений,

теории индексов целых комплексных чисел. Дан анализ понятия полной системы счисления остаточных классов на комплексную область и подхода к разработке машинных алгоритмов в этих системах счисления. Книга предназначалась для математиков, работающих в области теории математических машин и их применения, и для инженеров — разработчиков цифровых вычислительных машин.

2. «Теоретические основы машинной арифметики»

Его фундаментальные исследования по природе машинной арифметики легли в основу оригинальной монографии издательства «Наука» Казахской ССР «Теоретические основы машинной арифметики» объёмом 17 печатных листов и тиражом 1150 экземпляров, которая увидела свет в 1976 году. Впервые в монографии рассматривалась машинная арифметика как новая дисциплина, возникшая на стыке методов инструментального счета, теории кодирования, теории точности вычислительных методов организации вычислений. По мнению автора, прогресс в создании и широком использовании вычислительной техники в немалой степени зависит от решения двух проблем: проектирования вычислительных средств на новой технологической и элементной базе и проектирования систем вычисления на основе широкого привлечения математических конструкций и концепций. Проектирование систем вычислений как научное направление включает в себя много актуальных проблем современной прикладной математики. Монография знакомит с двумя из них, связанными с задачами кодирования. Первая формулируется как «разработка системы дискретных аппроксимационных моделей вещественных чисел и математических объектов более сплошной природы, чем числа», вторая — «разработка системы кодирования элементов дискретных моделей верхнего и нижнего уровней в форме, удобной для задач автоматизации и повышения надёжности вычислений». Кроме того, автором освещаются методологические вопросы построения дискретных аппроксимационных моделей вещественных чисел и математических моделей более общей природы, рассматриваются вопросы кодирования элементов конечных дискретных моделей, непозиционные арифметические

коды, вводится понятие диапазона на случай кольца главных идеалов, обсуждаются вопросы арифметического кодирования функциональных объектов. В монографии Вильжан Мавлютинович впервые проводит фундаментальный анализ понятия диапазона и арифметического кодирования. Достойное место занимает разработка новых алгоритмических приёмов повышения эффективности выполнения немодульных операций в непозиционной системе счисления.

3. «Операционное исчисление и обобщённые ряды Лагерра»

В 1974 г. в издательстве «Наука» вышла монография В. М. Амербаева «Операционное исчисление и обобщённые ряды Лагерра» объёмом 11,5 печатных листов. В ней излагается новый подход к построению операционного исчисления, сущность которого заключается в разработке процедур, расширяющих область определения операторов. В качестве аппарата автор использует обобщённые ряды Лагерра и метод аналитического продолжения функций комплексного переменного. В монографии рассматриваются три стержневые проблемы, возникающие в связи с обобщением операционного исчисления: *первая* — распространение операционных правил на класс обобщённых оригиналов, *вторая* — изучение состава пространства обобщённых оригиналов и *третья* — исследование алгоритмов и приёмов построения неизвестного оригинала, когда известно изображение. Монография состоит из шести глав. В первой главе автор ставит цель показать идейное родство дискретного и непрерывного операционных исчислений, проиллюстрировать на примере дискретных преобразований силу эйлеровских идей по обобщению понятия суммы расходящихся рядов, подготовить идейный фундамент, ввести понятие обобщённого ряда Лаггера для последующего обобщения операционного исчисления.

4. «Параллельные вычисления в комплексной плоскости»

Несмотря на географическое отдаление, Вильжан Мавлютинович продолжал активно сотрудничать с Казахстаном. По-прежнему под руководством Вильжана Мавлютиновича и мэтра модулярной арифметики И. Я. Акушского в Институте математики проводились исследования по модульной арифметике

комплексных чисел. Результатом этих исследований стал выход в 1984 году в издательстве «Наука» в соавторстве со мною монографии «Параллельные вычисления в комплексной плоскости» объёмом 10,7 листов и тиражом 1000 экз. Монография является продолжением книги «Основы машинной арифметики комплексных чисел», упомянутой выше. Опираясь на принятую в этой книге координатную форму представления комплексных чисел, авторы новой монографии представили исследования специфических вопросов кодирования комплексных чисел, способов машинной реализации, проанализировали различные аспекты применения разрабатываемой теории для повышения эффективности обработки комплекснозначной информации. По существу, монография является итогом многолетней работы авторов по созданию теории и практики эффективного кодирования комплексной информации. Под эффективностью кодирования комплексной информации понимается такая особенность кодирования комплексных величин, которая позволяет:

во-первых, так организовать вычисления в поле комплексных чисел, что создаются выигрыш временных затрат, экономия ёмкостей оперативных запоминающих устройств и повышается надёжность вычислений при заданных ограничениях на точность вычислений,

во-вторых, открывается возможность применения предложенных кодов для хранения, передачи и обработки большого потока планарной информации, чтобы обеспечить основы построения регулярных методов создания реконфигурационной арифметики и на этой основе повысить процент выхода годных кристаллов арифметических процессов в микроэлектронном производстве.

Монография состоит из двух частей.

Первая часть (три главы) посвящена разработке теории и методов модулярной арифметики комплексных чисел. В ней рассматриваются вопросы градуирования и шкалирования комплексных величин, понятие машинного диапазона, а также распространение режимов вычислений с фиксированной и плавающей запятой на комплексные числа; излагаются основы теории сравнений целых комплексных чисел (гауссовых

чисел), раскрывается алгебраическая структура машинного диапазона. Кроме того, показано, что поскольку комплексные числа не наделены отношением порядка (подобно вещественным числам), то преимущества позиционного кодирования комплексных чисел ослабляются. Вместе с тем авторы считают, что приведённые в первой части анализы принципов позиционного кодирования комплексных чисел оригинальны и представляют самостоятельный интерес для теории и практики вычислений комплексных чисел. Детально рассматривается модулярная арифметика комплексных чисел, в которой достигнута существенная эффективность машинной реализации алгоритмов немодульных операций благодаря использованию попарно взаимно простых комплексно-сопряжённых оснований. Дано определение гауссовой арифметики как арифметики кольца вычетов гауссовых чисел по составному модулю, состоящего из попарно взаимно простых комплексно-сопряжённых целых гауссовых чисел. Все вычислительные процедуры в этой арифметике реализуются в классе вещественных вычетов по вещественным модулям.

Вторая часть книги (четвёртая глава) посвящена новым приложениям гауссовой арифметики. Показано, что в гауссовой арифметике эффективно распараллеливаются вычислительные процедуры, связанные с решением многих практических задач: в частности, при специальном выборе оснований она распараллеливает теоретико-числовое быстрое преобразование Фурье, что существенно ускоряет процесс вычисления свёрток и корреляционных функций и обеспечивает гарантированную точность вычислений. Рассмотрены два варианта распараллеливания БПФ тригонометрического базиса в гауссовой арифметике, основанных на представлении БПФ в виде циклических свёрток. Показано также, что фундаментальные операции линейной алгебры — скалярное произведение векторов, умножение матрицы на вектор, умножение матрицы на матрицу — представляют класс процедур, допускающих эффективную реализацию в гауссовой арифметике. Большая эффективность достигается в гауссовой арифметике при решении алгебраических систем высокого порядка итерационными методами.

5. «Численный анализ лагерровского спектра»

Вильжан Мавлютинович со своим учеником Н. А. Утембаевым, продолжая исследования по одной из своих «старых» тематик, получили оригинальные результаты по численному анализу обращения преобразования Лапласа, опубликованные в вышедшей в 1982 г. в издательстве «Наука» Казахской ССР монографии «Численный анализ лагерровского спектра» объёмом 10,9 печатных листов и тиражом 1000 экземпляров. Монография посвящена исследованиям вопросов связи рядов Лагерра с широким классом интегральных преобразований, а также построению численных алгоритмов и приёмам восстановления оригинала на базе методов гармоничного анализа. Кроме того, в ней описаны сходимости численных алгоритмов и устойчивость суммирования рядов Лагерра. Часть монографии отводится вопросам приложения лагерровского спектра для решения конкретных прикладных задач.

6. «Распределение регулярных потоков сообщений в информационных системах»

В монографии «Распределение регулярных потоков сообщений в информационных системах» (изд. «Наука», 1980, соавторы В. И. Васильев, И. М. Гуревич, И. Т. Пак) рассматривается распределение регулярных, в том числе периодических, потоков, сообщений в центрах коммутации каналов связи больших информационных систем. В книге поставлена и рассмотрена задача детерминированного временного распределения регулярных потоков в информационных системах. Приводятся примеры практического использования разработанных методов.

В монографиях Вильжан Мавлютинович обобщал результаты своих исследований в определённых направлениях математики, подводил итог определённому этапу исследований.

Но был ещё факт, в котором чётко проявились и роль В. М. Амербаева в развитии отечественной вычислительной математики, и его авторитет среди учёных страны, и государственное признание его заслуг. Это присуждение ему в 1991 г. Государственной премии СССР «*За разработку и внедрение в народное хозяйство систем измерения позиционно-модулярного*

типа». Непосредственного участия в этой разработке Вильжан Мавлютинович не принимал. Но он был в постоянном контакте с учёными-модулярщиками страны, был в курсе их дел и, при необходимости, консультировал и подсказывал пути решения возникающих проблем. Поэтому участники разработки А. А. Коляда (из Белоруссии) и М. В. Синьков (из Украины) сочли невозможным не указать В. М. Амербаева при подготовке наградных документов. Для Вильжана Мавлютиновича это был неожиданный, но приятный подарок.

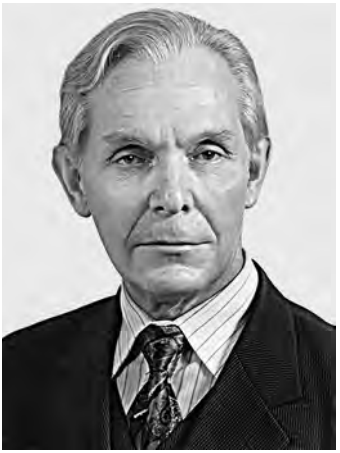
Меня всегда поражала удивительная доброта Вильжана Мавлютиновича, который своими поступками и поддержкой оказал многим действительную помощь и который всегда старался не причинять никаких неудобств окружающим его людям, будь то коллеги, друзья, ученики.

Подготовлено для настоящего сборника

Выступление в музее ОАО «Ангстрем»

Научно-производственная деятельность В. М. Амербаева в Зеленограде

Малашевич Б. М.



Малашевич
Борис Михайлович

В Зеленоград, а точнее в создаваемый в нём Минэлектронпромом СССР (МЭП) общесоюзный инвестиционный Центр микроэлектроники, В. М. Амербаев попал январе 1966 г. по приглашению Д. И. Юдицкого и И. Я. Акушского.

В это время они разрабатывали высокопроизводительную модулярную (на основе системы остаточных классов — СОК) ЭВМ и нуждались в хорошем математике для разработки алгоритмов выполнения модулярных операций. Их выбор пал на молодого Вильжана Амербаева, практически продемонстрировавшего на семинаре и свою заинтересованность модулярной арифметикой, и способность решать её проблемы нетривиальными методами.

В результате с 6 января 1966 г. он приступил к работе в качестве старшего научного сотрудника зеленоградского предприятия п/я 2014 (НИИ физических проблем — НИИФП).

Модулярная арифметика супер-ЭВМ

Проект «Алмаз»

Здесь Вильжан Мавлютинович, ранее чистый теоретик, впервые окунулся в практическую, прикладную вычислительную математику, принял участие в разработке технического проекта супер-ЭВМ[1], производительность которой значительно превосходила всё известное тогда не только в стране, но и в мире.

[1] Под супер-ЭВМ понимается ЭВМ с рекордно высокой для своего времени производительностью.

Разработка супер-ЭВМ производилась по специальному постановлению ЦК КПСС и СМ СССР, предусматривавшему создание второй очереди системы противоракетной обороны (ПРО) А-35 московского промышленного района (генеральный конструктор Григорий Васильевич Кисунько, директор ОКБ «Вымпел»). Тогда это была одна из важнейших задач общегосударственного значения.

К этому времени боевая система А-35 была уже практически разработана, в значительной степени изготовлена и частично смонтирована на боевых позициях. Но в США появились межконтинентальные баллистические ракеты (МБР) с разделяющимися (кассетными) боеголовками. А-35 с моноканальными стрельбовыми комплексами бороться с такими МБР не могла — в своё время её заказчики не смогли предвидеть появление кассетных боеголовок и не заложили соответствующих требований к системе. Было принято решение о модернизации А-35 и о создании её второй очереди, дополняющей А-35 тремя принципиально новыми многоканальными стрельбовыми комплексами (МКСК). Были начаты разработка и изготовление их полигонного варианта — МКСК «Аргунь». Главным конструктором (ГК) МКСК «Аргунь» Г. В. Кисунько назначил Николая Кузьмича Остапенко.

По предварительным оценкам, для МКСК требовалась ЭВМ с производительностью около 3,0 млн алгоритмических оп/с. Как вспоминал Н. К. Остапенко, «*одна алгоритмическая операция на задачах МКСК соответствовала примерно 3–4 коротким операциям ЭВМ*», т. е. в обычном тогда понимании требовалась ЭВМ с быстродействием около 10 (9–12) млн оп/с. Такой ЭВМ тогда на Земле не существовало. Лучшие известные на конец 1967 г. ЭВМ обладали быстродействием, в 4–12 раз меньшим требуемого для МКСК (таблица подготовлена в 1968 г. Д. И. Юдицким):

Фирма	Модель	Быстродействие сложений/с	Быстродействие элементов
IBM	360/75	1,0 млн	5 нс
CDC	6600	2,5 млн	10 нс
Philco	2000/212	1,5 млн	5 нс
Burroughs	B 5500	0,3 млн	20 нс
Sparry Rand	1108	1,2 млн	5 нс

Когда требования к ЭВМ прояснились, встал вопрос о том, где её взять. В это время готовилось постановление ЦК КПСС и СМ СССР по развитию ПРО, вышедшее 5 ноября 1965 г. В него и включили трём предприятиям (ЦМ (МЭП, Ф. В. Лукин), ИТМиВТ (МРП, С. А. Лебедев) и ИНЭУМ (Минприбор, М. А. Карцев)) конкурсное задание на разработку для «Аргуни» эскизных проектов высокопроизводительной ЭВМ со сроком окончания 30 марта 1967 года.

Так в Зеленограде под руководством директора ЦМ Фёдора Викторовича Лукина началась разработка эскизного проекта супер-ЭВМ «Алмаз», главным идеологом построения ЭВМ, практически главным конструктором был Д. И. Юдицкий.

Построить требуемую ЭВМ на традиционной двоичной позиционной системе счисления на технических средствах того времени было невозможно, о чём свидетельствует и приведённая выше таблица. Но Д. И. Юдицкий и ядро его коллектива уже имели опыт построения модулярной супер-ЭВМ К340А на основе непозиционной системы счисления остаточных классов (СОК), обеспечивающей распараллеливание выполнения операций на уровне операндов и, тем самым, в разы более высокую производительность. Машина (К340А) уже работала, разворачивалось её серийное производство.

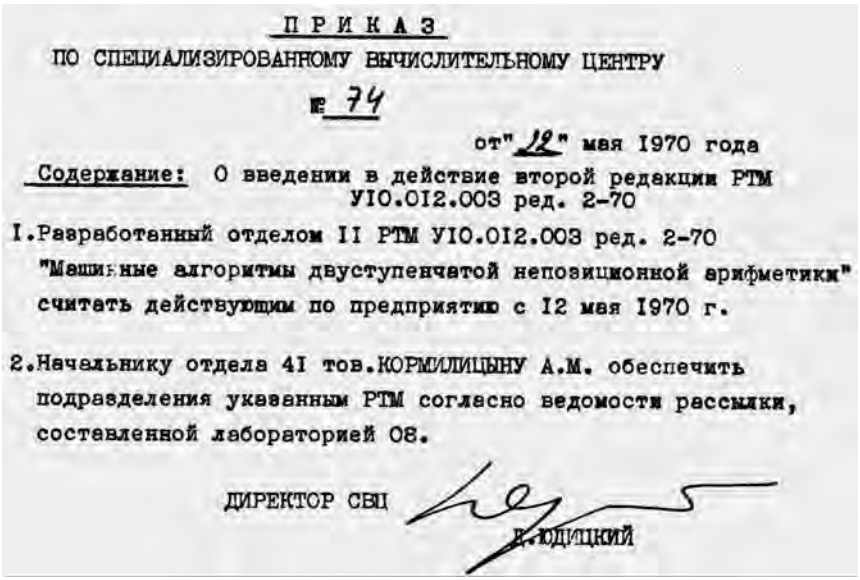
Но это было первое в мире применение модулярной арифметики в мощной супер-ЭВМ, её версия требовала существенной доработки на основе углублённого изучения этой новой области вычислительной математики. Вот это изучение и разработка практически реализуемых модулярных алгоритмов и стали основной задачей Вильжана Мавлютиновича и вверенного ему небольшого коллектива.

И Вильжан Мавлютинович с честью выполнил поставленную задачу, непосредственно сотрудничая с разработчиками процессора. Как вспоминает участник этих работ системотехник М. Д. Корнев, «*ночью Вильжан Мавлютинович думает, утром результаты приносит В. М. Радунскому* (начальнику отдела разработчиков). *Схемотехники просматривают аппаратную реализацию нового варианта, задают Амербаеву вопросы, он*

уходит думать опять, и так до тех пор, пока его идеи не поддадутся хорошей аппаратной реализации». Это характерный пример взаимодействия подразделений и специалистов СВЦ в ходе разработки 5Э53. А для Вильжана Мавлютиновича — хорошая школа, научившая его всегда думать о практической реализуемости результатов теоретических разработок.

Вильжаном Мавлютиновичем была создана значительно более совершенная версия модулярной арифметики, отличающаяся:

- хорошей практической схемотехнической реализуемостью,
- высочайшей по тем временам производительностью и надёжностью вычислений,
- способностью обнаруживать двойные и исправлять одинарные ошибки в процессе вычислений (что тогда не умели иные системы счисления),
- минимизацией аппаратурных средств и др.



ПРИКАЗ

ПО СПЕЦИАЛИЗИРОВАННОМУ ВЫЧИСЛИТЕЛЬНОМУ ЦЕНТРУ

№ 74

от "12" мая 1970 года

Содержание: О введении в действие второй редакции РТМ У10.012.003 ред. 2-70

1. Разработанный отделом 11 РТМ У10.012.003 ред. 2-70 "Машинные алгоритмы двуступенчатой непозиционной арифметики" считать действующим по предприятию с 12 мая 1970 г.

2. Начальнику отдела 41 тов. КОРМИЛИЦЫНУ А.М. обеспечить подразделения указанным РТМ согласно ведомости рассылки, составленной лабораторией 08.

ДИРЕКТОР СВЦ Б. ЮДИЦКИЙ

Приказ СВЦ о внедрении РТМ У10.012.003 2-70
о двухступенчатом СОК

Итог этой работы был сформулирован в виде двух документов:

- отчёта «Математическое обоснование машинных алгоритмов ЦВМ», Москва, СВЦ, 1969 г.,
- «Руководящего технического материала» РТМ У10.012.003 ред. 2-70 «Машинные алгоритмы двухступенчатой непозиционной арифметики», Москва, СВЦ, 1970.

Вот что с учётом результатов работы Вильжана Мавлютиновича писал Д. И. Юдицкий в итоговой справке по проекту «Алмаз» в марте 1968 г.:

«*В результате проведённых исследований было установлено, что в непозиционных системах могут быть построены самокорректирующиеся коды, позволяющие восстанавливать истинные результаты вычислений по цепи элементарных операций, если во время этих вычислений имели место какие-либо искажения.*

Была построена теория специального кодирования в непозиционных системах, позволяющая введением минимальной избыточности в представление слова осуществлять исправление возникающих ошибок методами, близкими к исправлению по смыслу на основе анализа последовательно получающихся слов в процессе обработки.

Применение методов специального кодирования значительно увеличивает функциональную надёжность вычислительных машин и позволяет создавать «живучие» машины, сохраняющие работоспособность при выходе из строя значительной части оборудования.

Таким образом, требования генерального конструктора оказалось возможным удовлетворить:

1) за счёт использования разработанной в научном центре теории непозиционных систем исчисления, позволяющей добиваться высокой производительности на основе широкого распараллеливания выполнения элементарных операций и максимальной надёжности в силу специфических самокорректирующихся способностей непозиционных систем;

2) за счёт использования микроэлектронной технологии изготовления системы логических элементов и основных блоков и узлов вычислительной машины, удачно сочетающейся со спецификой непозиционных систем».

Инженерный пульт управления ЭВМ «Алмаз»

Эскизный проект супер-ЭВМ «Алмаз» был разработан и 30 марта 1967 г. представлен заказчику. В результате рассмотрения проектов он и выиграл конкурс.

Проект 5Э53

В результате 20 мая 1968 г. ОКБ «Вымпел» и НЦ заключили договор на разработку высокопроизводительной ЭВМ 5Э53 и 5-машинного вычислительного комплекса на её основе с организацией серийного производства на Загорском электромеханическом заводе (ЗЭМЗ) Минрадиопрома и сдачей сокращённого 4-машинного комплекса на балхашском (Сары-Шаган) противоракетном полигоне в составе МКСК «Аргунь». Главным конструктором 5Э53 был назначен Д. И. Юдицкий.

А в октябре 1969 г. коллектив разработчиков ЭВМ был выделен в самостоятельное предприятие — специализированный вычислительный центр (СВЦ), директором был назначен Д. И. Юдицкий, и.о. зам. по науке — И. Я. Акушский. В. М. Амербаев стал начальником отдела вычислительной математики и продолжил работу по совершенствованию версии модулярной арифметики для повышения её эффективности и улучшения аппаратной реализуемости.

Появилась и новая задача — создание табличной модулярной арифметики (результаты операции не вычисляются, а извлекаются из таблицы) для реализации ЭВМ следующего, 4-го поколения (проект ЭВМ-IV) производительностью 200 млн оп/с, на основе появляющихся больших интегральных схем (БИС).

О проекте 5Э53 В. М. Амербаев вспоминал: «*Главным конструктором изделия 5Э53 Ф. В. Лукин назначил Д. И. Юдицкого, поручив ему руководство специализированным вычислительным центром. Давлет Исламович был истинным главным конструктором. Он вникал во все детали разрабатываемого проекта — от технологии производства новых элементов до структурных решений, архитектуры ЭВМ и математического обеспечения. На всех участках своей напряжённой работы он умел ставить такие вопросы и задачи, решение которых приводило к созданию новых оригинальных блоков конструируемого изделия, а в ряде случаев Давлет Исламович сам указывал подобные решения. Давлет Исламович работал сам, не считаясь ни со временем, ни с обстоятельствами, так же как и все его товарищи по труду. Это было бурное и яркое время, и, конечно, центром и организатором всего был Давлет Исламович. Проект изделия был разработан к сроку. В процессе этой работы Давлет Исламович не оставлял исследовательской работы. Им была разработана общая теория живучести вычислительных средств (впоследствии они получили названия отказоустойчивых систем) и даны технические решения отдельных положений этой теории, которые нашли отражение в проекте 5Э53*».

Применение разработанной Вильжаном Мавлютиновичем версии модулярной арифметики обеспечивало два основных бесспорных преимущества 5Э53:

- повышенную производительность и простоту аппаратной реализации арифметического устройства за счёт малой разрядности оснований СОК,
- повышенную надёжность системы благодаря свойствам СОК, обеспечивающим обнаружение и исправление ошибок, возникающих при выполнении операций

в арифметическом устройстве (двоичные ЭВМ этого никогда не умели).

Параллельно с выполнением проектов 5Э53 и ЭВМ-IV СВЦ во главе с И. Я. Акушским стало общепризнанным центром развития модулярной арифметики в стране.

Главными теоретиками СОК в стране были Д. И. Юдицкий, И. Я. Акушский[2], В. М. Амербаев и их ученики. Основные положения теории СОК, создаваемые в СВЦ и за его пределами, были сформулированы ими в многочисленных статьях и монографиях. В частности, И. Я. Акушским, В. М. Амербаевым и их учениками были разработаны методы проведения вычислений в супербольших диапазонах с числами в сотни тысяч разрядов. Это определило подходы к решению ряда вычислительных задач теории чисел, остававшихся нерешёнными со времён Эйлера, Гаусса, Ферма.

В целом работы СВЦ по модулярной арифметике, по обобщению СОК на различных классах математических объектов примерно на десять лет опережали зарубежный уровень.

А результаты работ В. М. Амербаева также нашли отражение в статьях, выступлениях на научных конференциях и в монографиях, а также в его докторской диссертации на тему «*Вычисления в кольце главных идеалов и их приложения в вычислительной технике*», которую он защитил в 1971 г. на учёном совете зеленоградского НПО «Элас».

В диссертации была разработана алгебраическая концепция параллельных вычислений и повышения надёжности вычислений посредством алгебраических методов введения избыточности, принципы арифметического самокорректирующегося кодирования. Частные реализации этой концепции

---

[2] Широко распространено мнение, что в паре Юдицкий — Акушский лидером был И. Я. Акушский. Четыре факта опровергают это. 1. Юдицкий имел систематизированное высшее математическое образование, Акушский — фрагментное, «полученное самообразованием». 2. Юдицкий всегда был начальником Акушского. 3. Главным конструктором разработок всегда назначали Юдицкого, Акушский был участником разработки. 4. Авторитет Юдицкого в коллективе всегда был существенно выше.

легли в основу проектирования арифметического процессора высокопроизводительной вычислительной системы 5Э53.

Проект 5Э53 был завершён успешно и в срок.

27 февраля 1971 г. восемь комплектов конструкторской документации (по 97 272 листа каждый) колонной машин были доставлены на ЗЭМЗ. Началась подготовка производства.

Но в это время в Минрадиопроме проводилось планомерное сворачивание разработки МКСК «Аргунь», для которого 5Э53 предназначалась. Для 5Э53 это закончилось приказом замминистра МРП о прекращении финансирования ЦНПО «Вымпел» для завершения работ по договору с СВЦ о создании 5Э53 и работ по организации производства 5Э53 на ЗЭМЗ. Для ЭВМ это был смертельный приговор.

Как свидетельствует Н. К. Остапенко, «*к концу 1971 г. все оборудование «Аргуни» было смонтировано и отлажено, недоставало лишь противоракеты (ПР) А-351 и ЭВМ 5Э53. В этих условиях, когда Загорский электромеханический завод уже начал изготовление устройств 5Э53, финансирование работ по ЭВМ и ПР руководством МРП было прекращено, а договоры затем расторгнуты. К началу 1973 г. создание МКСК «Аргунь» было полностью прекращено, готовые стартовые позиции противоракет взорваны, РКИ-35ТА* (РЛС наведения противоракет) *демонтирована и отправлена в Киевскую военную академию, многие системы физически урезаны. Уникальный и перспективный стрельбовый комплекс «Аргунь», подобного которому ещё более 20 лет не было на земле, превратили в многоканальный измерительный комплекс (МИК) «Аргунь-И», тоже превосходящий существующие образцы, но весьма далёкий от заложенных в нем возможностей. Вот пример: с ЭВМ 5Э53 МКСК «Аргунь» мог отслеживать более 100 элементов сложных баллистических целей, а МИК «Аргунь-И» с ЭВМ 5Э92б, применённых вместо 5Э53, — только 13*».

Г. В. Кисунько был освобождён от обязанностей генерального конструктора ПРО и переведён на работу на другое предприятие. Н. К. Остапенко был вынужден покинуть ОКБ «Вымпел» и оказался в СВЦ.

Таким образом, перспективный проект супер-ЭВМ 5Э53 был погублен. А её экспериментальный образец, изготовленный

опытным производством СВЦ, отправился в Алма-Ату, в Институт физики высоких энергий АН Казахстана для обсчёта треков частиц в камере Вильсона, на этих задачах специфика 5Э53 обещала высокую эффективность. Но без авторского сопровождения со стороны разработчиков освоен он там так и не был.

Загублена была не только 5Э53.

Было пресечено новое перспективное направление развития отечественной вычислительной техники, превосходящее всё имевшееся и в стране, и за рубежом. Истинных причин провала проекта супер-ЭВМ на основе СОК из-за его секретности практически никто не знал. Но сам факт, получив широкую огласку в кругах специалистов, начал самостоятельную жизнь и стал почти непреодолимым барьером на дальнейшем пути внедрения СОК в отечественную вычислительную технику. Далее модулярной арифметикой в нашей стране занимались только отдельные энтузиасты, в основном в учебных и академических институтах и, соответственно, исключительно в теоретическом плане.

За этот период В. М. Амербаевым опубликовано 24 научных труда, в т. ч. монография и два авторских свидетельства на изобретение.

На таком фоне Вильжан Мавлютинович получил предложение АН КазССР занять должность заместителя директора Института математики и механики АН КазССР, к становлению которого он ранее имел непосредственное отношение. Там он проработал с 14.03.1972 г. по 01.02.1977 г. Но резкое ухудшение здоровья супруги Эмилии Нестеровны потребовало смены высокогорного климата Алма-Аты (около 800 м над уровнем моря) на равнинный. Им пришлось возвращаться в Зеленоград.

Работа в вузах

К этому времени в Зеленоградском НЦ произошла крупная реорганизация, в результате которой СВЦ разделили на две части, а Д. И. Юдицкий и многие ведущие специалисты покинули научный центр. Оставшиеся разработчики СВЦ, сначала переведённые в НИИ точной технологии (НИИТТ), а затем — в НИИ

«Научный центр» (НИИНЦ), разрабатывали микропроцессоры, микро-ЭВМ и микросистемы. Все они были 16-разрядные, а на малой разрядности СОК неэффективен (он именно потому эффективен, что разбивает многоразрядные операнды на малоразрядные). О модулярной арифметике в Зеленограде вспоминали только ветераны — участники разработки 5Э53 и ЭВМ-IV.

Других интересных для В. М. Амербаева математических задач на предприятиях Зеленограда тогда не обнаружилось, и Вильжан Мавлютинович перешёл на преподавательскую работу. Сначала в Московский институт инженеров гражданской авиации (МИИГА) в качестве заведующего кафедрой «Электронные вычислительные машины», а затем в зеленоградский филиал Московского института электронной техники (МИЭТ) в качестве профессора кафедры высшей математики. На этом этапе основными его занятиями были преподавание высшей математики студентам, работа с аспирантами и фундаментальные исследования в вычислительной математике.

За этот 11-летний педагогический период В. М. Амербаевым опубликовано 39 научных трудов, в т. ч. 4 монографии и 13 авторских свидетельств на изобретения.

В 1988 г. В. М. Амербаев был вторично приглашён для работы в Алма-Ату в качестве академика АН КазССР и академика-секретаря отделения физико-математических наук АН КазССР. Там он проработал с 18.07.1988 по 14.07.1994 гг., но затем вернулся в Зеленоград.

В 1994–2002 гг. В. М. Амербаев работал в МИЭТе в должности профессора. Результаты его работ нашли отражение в 19 публикациях.

Вот как о педагогической деятельности Вильжана Мавлютиновича в МИЭТе рассказывают профессор Кожухов Игорь Борисович и доцент Александр Михайлович Ревякин:

«*Приход в 1994 г. В. М. Амербаева существенно активизировал научную работу в МИЭТе. В частности, на кафедре высшей математики появились студенты и аспиранты ещё одной научной школы — школы Амербаева. До этого преобладающим научным направлением на кафедре был математический анализ — направление заведующего кафедрой профессора А. В. Ефимова*

и профессоров Я. С. Бугрова и П. К. Суэтина. Вильжан Мавлютинович основал направление теоретических основ проектирования вычислительных устройств. Его широкая эрудиция позволила использовать в этих вопросах методы современной алгебры и дискретной математики. Ряд учеников Амербаева успешно защитили кандидатские диссертации. В. М. Амербаев входил в диссертационный совет при МИЭТе, где представлял математические и технические специальности, связанные с созданием вычислительных устройств.

В начале 2000-х В. М. Амербаев создал творческую группу для разработки математических методов в вопросах передачи и переработки информации. Работа группы была поддержана Российским фондом фундаментальных исследований (РФФИ РФ), руководителем темы был назначен Вильжан Мавлютинович.

Научная работа В. М. Амербаева не ограничивалась МИЭТом. Он сотрудничал с различными предприятиями, редколлегиями научных журналов, участвовал в работе диссертационных советов. Он взаимодействовал с Московской государственной академией делового администрирования (МГАДА), где курировал специальности, связанные с защитой информации, руководил курсовыми и дипломными работами студентов. Научный журнал «Вестник МГАДА» посвятил целиком один из своих номеров работам В. М. Амербаева, его коллег и учеников.

Педагогическая деятельность профессора В. М. Амербаева отличалась высоким научным уровнем преподавания и творческим подходом. Он читал курсы лекций по различным разделам математики и её приложений, вычислительной техники, будучи профессором кафедры высшей математики, а затем кафедры вычислительной техники. Это линейная алгебра и дифференциальные уравнения для первокурсников, теория кодирования и шифрования для студентов старших курсов и т. д. Тот период — рубеж XX и XXI веков — для кафедры высшей математики (а наверное, и для других кафедр) характеризовался существенным изменением спектра изучаемых предметов. Появились новые, ранее в МИЭТе не читавшиеся дисциплины — например дискретная математика. Здесь очень пригодились знания профессора Амербаева, который с энтузиазмом занялся разработкой методики

преподавания этих дисциплин. Впоследствии к этим дисциплинам добавились математические и инженерные науки, связанные с защитой информации, теорией нейронных сетей, и здесь снова оказались очень кстати высокие профессиональные качества В. М. Амербаева и его способность быстро включать в свой арсенал знаний новые разделы науки. В описываемый период времени случилось ещё одно знаменательное для математической кафедры событие — сбылась мечта заведующего кафедрой профессора А. С. Поспелова об открытии на кафедре специальности «прикладная математика». Конечно, это была мечта не одного Поспелова, а многих сотрудников кафедры. Вильжан Мавлютинович активно помогал заведующему кафедрой в реализации этой идеи. Следует отметить, что кафедра при этом стала выпускающей, у неё появились студенты-дипломники, и одним из наиболее активных научных руководителей стал профессор В. М. Амербаев. Необыкновенная широта эрудиции В. М. Амербаева и его безграничная любовь к студентам позволили донести до учащихся понимание самых сложных разделов науки и вырастить высококвалифицированных специалистов.

Вильжан Мавлютинович всегда высоко ценил молодёжь. Он участвовал в организации и проведении творческих конкурсов школьников Зеленограда.

Вильжан Мавлютинович — человек широчайшей души, добрый и отзывчивый. Благодаря этому он пользовался большим уважением преподавателей и студентов».

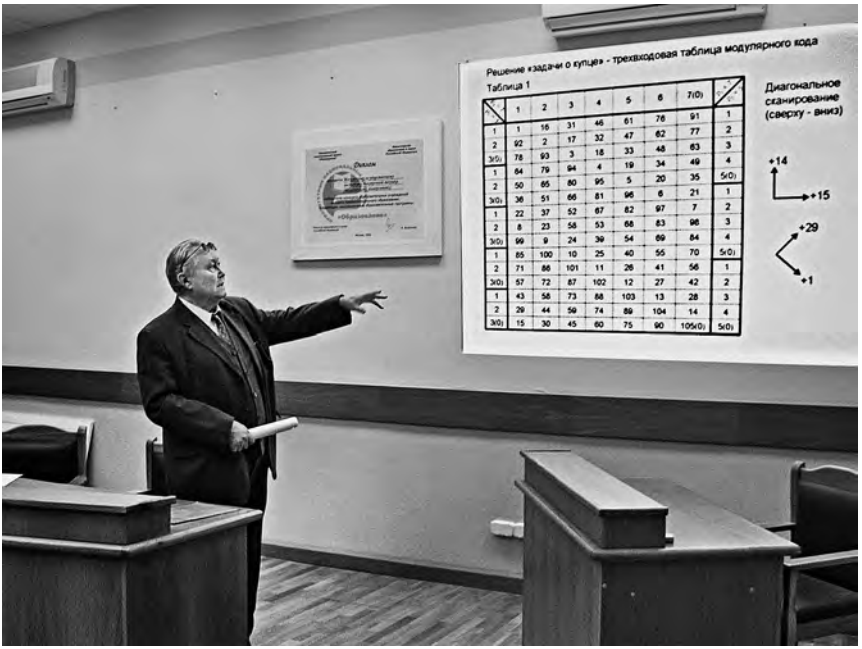
Всего Вильжан Мавлютинович течение 29 лет преподавал студентам МИЭТа высшую математику, вёл научную работу.

При работе в МИЭТе и других предприятиях спектр научных интересов Вильжана Мавлютиновича никогда не ограничивался его служебными обязанностями. Вот примеры.

Приближался 2005 г., год 50-летия системы остаточных классов, предложенной в 1955 г. двумя чешскими учёными А. Свободой и М. Валахом.

В. М. Амербаев и Б. М. Малашевич предложили отметить юбилей специальной научно-технической конференцией. По общеизвестному правилу «*инициатива наказуема исполнением*» им и пришлось её организовывать. Получилась не просто

конференция, а «*юбилейная международная научно-техническая конференция "50 лет модулярной арифметики"*», в которой участвовали математики России, Казахстана, Белоруссии, Украины и США — всего 51 чел.



В. М. Амербаев на юбилейной конференции 11.12.2006

Вот ещё пример. Вильжан Мавлютинович всегда занимался и серьёзными фундаментальными исследованиями, «в свободном полёте» просматривая возможности новых применений модулярной арифметики и другие интересные для него направления вычислительной математики. Именно так он пришёл к применению модулярной арифметики в системах криптозащиты информации, к модулярной логарифметике и др.

В частности, в ОАО «Ангстрем» Вильжан Мавлютинович встретился с Николаем Петровичем Брусенцовым, который в конце 1960-х годов был главным конструктором троичных ЭВМ «Сетунь» (выпускалась серийно) и «Сетунь-70» (сделана

в одном экземпляре), работавших в троичной арифметике и трёхзначной логике. За истекшие годы, работая в МГУ, он серьёзно доработал троичную арифметику и трёхзначную логику на основе развитой им логики Аристотеля. В 2004–2005 гг. Н. П. Брусенцов предпринял попытку сделать на этой основе троичную ЭВМ, видя огромное её преимущество перед двоичными системами на ряде классов задач, особенно для создания искусственного интеллекта.

После обстоятельного разговора Вильжан Мавлютинович и Николай Петрович пришли к выводу о целесообразности попытки объединения положительных сторон модулярности и троичности. Состоялось несколько встреч, в т. ч. в МГУ, наметились некоторые предложения. Но резкое ухудшение состояния здоровья Николая Петровича (ему был 81 год) остановило эти работы. А без него (свои доработки троичности Н. П. Брусенцов не довёл до публикаций) идея оказалась нереализуемой.

Н. П. Брусенцов и В. М. Амербаев, МГУ, 2005 г.

Внедрение научных заделов

За годы работы в МИЭТе Вильжан Мавлютинович провёл глубокие научные исследования и получил серьёзные результаты в области вычислительной модулярной математики, доведя их до стадии пригодности к практической аппаратной реализации. Наступил момент их внедрения в предприятиях Зеленограда, разрабатывающих и производящих электронную аппаратуру, в которых нашлись интересные для него прикладные применения исследуемых им областей математики.

Защита информации

В результате В. М. Амербаев 18 декабря 2002 г. перешёл на должность главного научного сотрудника государственного унитарного предприятия «СПУРТ», продолжая преподавательскую и научную работу в МИЭТе по совместительству.

Здесь перед ним стояла задача математической проработки улучшения характеристик (быстродействие, надёжность, защищённость и др.) создаваемых в «СПУРТ» систем защиты информации.

Но в 2006 г. в «СПУРТ» было проведено уточнение тематики с соответствующей реорганизацией предприятия. Деятельность направления по защите информации была прекращена, а занимавшимся ею специалистам предложена работа в других подразделениях по другой тематике. Некоторые согласились, но далеко не все. А группа ведущих специалистов, в т. ч. и В. М. Амербаев, сконцентрировались в зеленоградской фирме «АНКАД», основной тематикой которой была именно защита информации.

Рассказать о научной и производственной деятельности Вильжана Мавлютиновича в «СПУРТ» и «АНКАД» попросим его коллегу Евгения Михайловича Зверева:

«*Амербаев В. М. и в «СПУРТ», и в «АНКАД» создавал истинно конкретную объективную атмосферу научности организации. Это заключалось в следующем. Он перевёл понятие «научно-техническая организация/предприятие» из формально красивого в конкретно полезное, наполненное научным содержанием.*

1. Активизировал научно-технический совет предприятия. Эти советы стали не формальными, а более активными и инициативными. Принимаемые решения носили неформальный характер и имели более высокую продуктивность. Практически все статьи, готовящиеся для печати, и тезисы докладов для НТ-конференций обсуждались на НТС предприятий. В частности, идеология статьи, помещённая в данной книге, с его участием в составе авторов обсуждалась на НТС «АНКАД» была положительно рекомендована НТС для дальнейшего её продвижения и реализации в конкретных ОКР. Её алгоритмические программно-временные решения были реализованы в конкретной структуре низовой радиосвязи заказчика. В «СПУРТ» в рамках учёного совета первая кандидатская защита состоялась по информационной безопасности его ученика по МИЭТу и (уже) коллеги по «СПУРТ» Шаромока А. В.

2. Он инициировал аспирантские подразделения (отдел аспирантуры). Организовал работу с аспирантами — читал лекции аспирантам, подвигал их на исследовательские деяния и написание НТ-статей со своим участием и без, инициировал их на участие в НТ-конференциях. Способствовал тому, чтобы молодые специалисты занимались преподавательской деятельностью. В частности, только из нашего подразделения, занимающегося ИТ-безопасностью, в МИЭТе на кафедре ТКС в разное время работали преподавателями 5–7 человек. Сам он не один год на той же кафедре был председателем ГАК. Кстати, о работе в ГАК: он категорически не любил ставить защищающимся дипломникам низкие оценки. Во многих случаях ему удавалось убеждать членов ГАК присоединиться к его более высокой оценке. Я это утверждаю как тоже многолетний член этой ГАК.

3. Сам Амербаев лично и в составе соавторов принимал участие в НТ-симпозиумах и конференциях внутреннего и международного уровней в интересах МО, ФСБ и негосударственных структур РФ (например «Рускрипто» и др.).

4. В «АНКАД» и МИЭТе организовывал НТ-встречи с учёными, в том числе и из ФСБ — с генерал-майором Кузьминым и рядом других видных специалистов. Его, Амербаева, имя в такой организации, как ФСБ, было весьма уважаемо.

5. Работая в подразделении создателей информационно-шифровальной техники, являлся там фактически собственным экспертом криптоматематических, алгоритмических, протокольных и программно-технических решений создаваемой аппаратуры. Его участие приводило к совершенствованию алгоритмов работы создаваемых устройств, к упрощению их аппаратной реализуемости и к улучшению характеристик шифротехники. Его участие в общей работе было отражено в целом ряде патентов».

Работе в «АНКАД», как было всегда в его жизни, Вильжан Мавлютинович отдавался полностью и выполнял её до последнего дня жизни.

Но работал он в нём «по совместительству», поскольку к моменту перехода из «СПУРТ» в «АНКАД» уже имел договорённость о поступлении на постоянную работу в ИППМ РАН, где принялся за решение принципиально новой задачи вычислительной математики.

Модулярная логарифметика

В модулярной арифметике очень быстро выполняются операции сложения и вычитания, но весьма громоздки умножения и деления. Это одна из главных проблем СОК, и на её решение направлены усилия всех занимающихся модулярной арифметикой учёных.

Но умножение чисел можно заменить сложением их логарифмов, если разработать соответствующий математический аппарат. Этими исследованиями, путями построения такого математического аппарата в СОК, т. е. модулярной логарифметикой, Вильжан Мавлютинович начал заниматься ещё в Алма-Ате. Проблема оказалась трудной, но интересной и разрешимой, такие проблемы он и любил.

И когда пути решения проблемы прояснились, Вильжан Мавлютинович познакомил с результатами академика РАН, директора зеленоградского Института проблем проектирования в микроэлектронике (ИППМ РАН) Александра Леонидовича Стемпковского.

Александр Леонидович сразу понял и принял идеи модулярной логарифметики, загорелся ими и предложил

В. М. Амербаеву должность главного научного сотрудника в ИППМ РАН. Тот с удовлетворением принял это предложение, оговорив продолжение работ по криптозащите информации в «АНКАД» и преподавания в МИЭТе.

На этих предприятиях он работал до последней отведённой ему судьбой секунды.

О работе В. А. Амербаева в ИППМ РАН рассказывает его ученик и продолжатель дела Дмитрий Владимирович Тельпухов:

«В ИППМ РАН Вильжан Мавлютинович привлекал толковых студентов МИЭТа на практику. Увлечённые его идеями, молодые люди по окончании института оставались работать в ИППМ, составляя костяк отдела, который возглавлял Вильжан Мавлютинович. Окружённый своими учениками, он активно занимался развитием интрамодулярных вычислений, к которым относятся вычисления на базе теоремы Гаусса об изоморфизме для обобщённых комплексных чисел и рекурсивная модулярная арифметика. Была сформулирована идея логарифметики и построенной на её основе бимодульной арифметики. В последние годы шла работа над идеей модулярного вычислительного элемента, на основе универсальной структуры которого предлагалось строить модулярное процессорное ядро без разделения на модульную и немодульные части. Работающие под его руководством студенты и аспиранты защищали диссертации и дипломные работы. При его активном участии защитили свои диссертации:

- *Семенов Михаил Юрьевич «Исследование и разработка методологии проектирования основных вычислительных узлов для устройств цифровой обработки сигналов в модулярной арифметике», кандидат технических наук, 2005,*
- *Ласточкин Олег Викторович «Исследование и разработка методов проектирования специализированных модулярных вычислительных блоков на основе автоматизированной генерации функциональных описаний», кандидат технических наук, 2007,*
- *Калашников Вячеслав Сергеевич «Исследование и разработка методов проектирования быстродействующих вычислительных узлов для реализации отказоустойчивых систем на основе модулярной арифметики», кандидат технических наук, 2007,*

• *Тельпухов Дмитрий Владимирович «Исследование и разработка прямых и обратных преобразователей кода модулярных вычислительных структур для устройств цифровой обработки сигналов», кандидат технических наук, 2012,*

• *Балака Екатерина Станиславовна «Исследование и разработка сбоеустойчивых устройств бимодульной модулярной арифметики», кандидат технических наук, 2014,*

• *Соловьев Роман Александрович «Микроэлектронные устройства цифровой обработки сигналов на базе модулярных вычислительных структур», доктор технических наук, 2018.*

В отделе, который возглавлял В. М. Амербаев, сложился симбиоз молодости и опыта, новых программных и вычислительных подходов, а также глубокой аналитической и теоретической базы, носителем которой был Вильжан Мавлютинович. В отделе публиковались статьи и оформлялись патенты, выполнялись научно-исследовательские работы и проводились семинары — шла настоящая творческая научная работа, в которой до самых последних дней Вильжан Мавлютинович Амербаев принимал самое активное участие».

Сейчас ученики Вильжана Мавлютиновича продолжают его дело с прекрасными результатами. Так, Дмитрий Тельпухов и Екатерина Балака по итогам конкурса 2015 г. за научно-исследовательскую работу «*Разработка микроэлектронных устройств цифровой обработки сигналов с применением математического аппарата системы остаточных классов*» награждены президиумом РАН медалями РАН и денежными премиями.

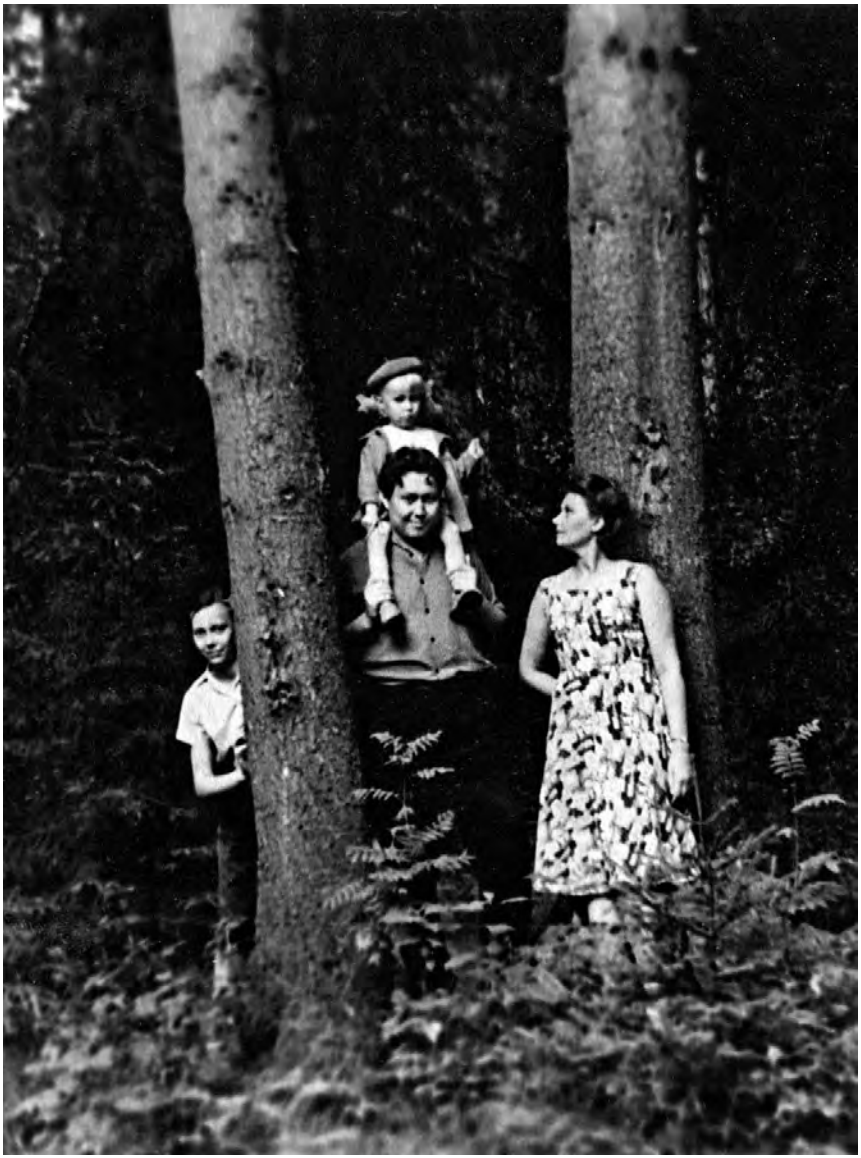
Заключение

Я неоднократно слышал от Вильжана Мавлютиновича, что модулярную арифметику он смог познать достаточно глубоко только на основе алгебры. В моём понимании человека, далёкого от математики, он говорил о своём главном методологическом подходе к изучению и развитию модулярной арифметики и её приложения к различным классам задач. Этим В. М. Амербаев коренным образом отличался от многих разработчиков

средств вычислительной техники, не оценивших и не применявших модулярную арифметику в своих системах. Они не смогли подняться выше арифметических подходов, и не увидели всех прелестей и возможностей модулярной арифметики, очевидных для Вильжана Мавлютиновича Амербаева.

В заключение не могу не сказать большое спасибо коллегам и ученикам В. М. Амербаева, оказавшим неоценимую помощь в освещении зеленоградского этапа его творческой деятельности: Звереву Евгению Михайловичу, Кожухову Игорю Борисовичу, Корневу Михаилу Дмитриевичу, Любушкиной Ирине Евгеньевне, Ревякину Александру Михайловичу, Тельпухову Дмитрию Владимировичу, Щёлокову Альберту Николаевичу.

Подготовлено для настоящего сборника



Ирина, Вильжан, Ольга (на плечах), Эмилия, 1967 г., Зеленоград

ГЛАВА 2

БИОГРАФИЯ В. М. АМЕРБАЕВА

Бурмистрова (Амербаева) И. В.,
Малашевич Б. М.

Вильжан Мавлютинович Амербаев — российский и казахстанский математик, доктор технических наук, профессор вычислительной математики, академик Национальной академии наук Республики Казахстан (ранее КазССР), лауреат Государственной премии СССР по науке и технике (1991 г.). Специалист в области компьютерной алгебры, теории арифметического кодирования информации, цифровой обработки сигналов и операционного исчисления.

Родители

Родился 25 апреля 1931 года в г. Талды-Кургане Казахской ССР.

Его отец, Амирбаев Мавлитдин[1] Оспанович (16.04.1908–16.10.1987) — из семьи ремесленника-портного.

Его мать Амирбаева (Чинибекова) Ашраф Ризаевна (29.12.1910–30.01.1991) родилась в семье богатого купца Ризы Чинибекова.

Молодой Мавлитдин работал батраком у купца Ризы, где и познакомился с его дочкой Ашраф. Они полюбили друг друга, однако никакой надежды получить разрешение её родителей на их брак не было. И в 1926 году молодые люди тайно сбежали из Талды-Кургана в Алма-Ату.

---

[1] При регистрации рождения Вильжана его дедушка Оспан сделал ошибки в фамилии (Амербаев, вместо Амирбаев) и в отчестве (Мавлютинович, вместо Мавлитдинович). Аналогичная история произошла с сестрой Вильжана Венерой и его женой Эмилией Несторовной. При выдаче паспортов они превратились в Винеру и Эмилию Нестеровну.

Родители Вильжана

Родители Вильжана с родственниками в Алма-Ате, 9 мая 1975 г.

Алма-Ата в 1930-е годы — главная Торговая (позже Горького) улица

Алма-Ата в 1930-е годы — Дворец труда

Алма-Ата в 1926 г. (до 3 марта 1921 г. — город-крепость Верный) была небольшим, ещё провинциальным, в основном одноэтажным городком.

Незадолго до их приезда город пережил два разрушительных природных бедствия:

• 4 января 1911 года в 04 часа 25 минут произошло катастрофическое Кеминское землетрясение с интенсивностью в эпицентре 10-11 баллов (магнитуда 8.2).

Последствия землетрясения 1911 г. в г. Верном

В городе Верном погибло около 50 человек, более сотни были ранены. Согласно актам оценочной комиссии, число совершенно разрушенных жилых домов достигло 616, требующих капитального ремонта — 301, домов с более лёгкими повреждениями фундаментов, печей и штукатурки — 1010, нежилых разрушенных построек — 3000, повреждённых — 2000.

• Летом 1921 года по реке Малая Алматинка селевой поток дошёл практически до центра города. Огромные булыжники перепахали целые кварталы. В течение пяти часов значительная часть Алма-Аты была превращена в руины и залита грязекаменной массой. Погибли более 500 человек.

И вот в этот истерзанный природой, но уже восстанавливающийся город, собирающийся стать столицей республики, приехали молодые Мавлитдин и Ашраф строить свою жизнь. Трудно было и городу, и им, но и город, и молодые победили невзгоды.


Улица Карла Маркса после селевого потока 8 июля 1921 г. и в 1973 г.

К сожалению, их первый сын Вилик (от «Владимир Ильич Ленин и Крупская», тогда подобные имена были популярны у прогрессивной молодёжи) умер при родах. И когда в 1931 году пришло время следующих родов, Ашраф уехала рожать к родителям в Талды-Курган. Вильжан был старшим ребёнком в семье. После него родились Винера, Наиля, Лейла, Варлен и Анвар. Все шестеро получили высшее образование.


Вильжан в детстве, справа с сёстрами Винерой и Наилёй

Своё первое образование на основе кириллического и арабского алфавитов Мавлитдин и Ашраф получили ещё в Талды-Кургане.

Винера, Наиля, Лейла, Варлен и Анвар

Здесь требуется пояснение.

Исторически казахи не имели своей письменности, образованная элита вместе с исламом приняла арабские язык и письменность. А затем стала использовать арабский алфавит для казахского языка (как народы западной Европы, приняв католицизм, пользовалась сначала латынью, а затем и до сих пор — латиницей). Но арабский алфавит плохо соответствовал богатой казахской фонетике, поэтому в 1912 году Ахмет Байтурсынов реформировал казахскую письменность на основе арабской графики, убрав все лишние арабские буквы, не соответствующие казахской фонетике, и добавив недостающие буквы, специфичные для казахского языка. Алфавит «Жана емле» («Новая орфография») содержит 29 букв и один надстрочный знак «хамза». Он и ныне используется казахами, проживающими в Китае, Афганистане и Иране.

В конце XIX в. была создана так называемая миссионерская кириллица, включающая 25 букв. Применялась до 1929 г. параллельно с «Жана емле».

С 1917 года в Казахстане начала набирать популярность идея латинизации. После длительного обсуждения в 1929 году казахский язык перешёл на латиницу. Обновлённый казахский алфавит насчитывал 30 букв с необходимыми добавлениями к ним знаков для передачи специфических звуков казахского языка. Но жизнь латинского письма в Казахстане была короткой — с 1929 по 1939 гг.

Новый алфавит 1940 года на основе русской кириллицы состоял из 42 букв и полностью учитывал фонетические особенности казахского языка.

26 октября 2017 года президент Казахстана Нурсултан Назарбаев подписал указ № 569 «О переводе алфавита казахского языка с кириллицы на латинскую графику» с поэтапным переводом алфавита казахского языка на латинскую графику до 2025 г.

Остаётся загадкой, почему казахстанские лингвисты примитивную 24-буквенную латиницу для фонетического богатого казахского языка предпочли 33-буквенной, дополненной до 42 букв кириллице, прекрасно освоенной в течение 77 лет несколькими поколениями казахов. А может быть, не лингвисты, а политики?

По прибытии в Алма-Ату Мавлитдин и Ашраф поступили на рабфак[2]. С рождением детей Ашраф вынуждена была бросить учёбу, хотя училась отлично. А Мавлитдин Оспанович благополучно закончил обучение и защитил диссертацию кандидата физико-математических наук.

Мавлитдин Оспанович Амирбаев, а затем и Вильжан Мавлютинович Амербаев, живя в Казахской ССР, но будучи татарами, принимали активное участие в становлении и развитии казахского народа, всего Казахстана, его образования, его науки. Мавлитдин Оспанович работал преподавателем высшей математики в Казахском педагогическом институте им. Абая (КазПИ) и в Казахском государственном университете им. С. М. Кирова (КазГУ), создавал первые в республике национальные учебники по математике, переводя их с русского языка на казахский на основе кириллического и арабского алфавитов. А Вильжан Мавлютинович был одним из ведущих создателей республиканской научной математической школы,

[2] Рабфак — «рабочий факультет» — общеобразовательное учебное заведение в 1919–1940 гг. в СССР для подготовки в высшие учебные заведения молодёжи, не имеющей среднего образования.

внёс огромный вклад в развитие вычислительной математики, защиты информации и информатизации республики.

КазГУ и КазПИ, в которых работал Мавлитдин Оспанович, имели общую историю, которая и определила его работу в обоих институтах. Первый университет в Казахстане был создан ещё в 1928 году. Однако достаточно быстро возникло понимание, что в те годы Казахстан прежде всего нуждался в учителях, поэтому вуз практически сразу был реорганизован в педагогический институт. В 1928–1929 учебном году в нём обучалось 124 студента, работало 9 преподавателей-профессоров.

Первое здание КазГУ, 1929 г.

В 1930 г. название вуза сменилось на «Казахский педагогический институт» (КазПИ), в 1935 г. ему было присвоено имя Абая.

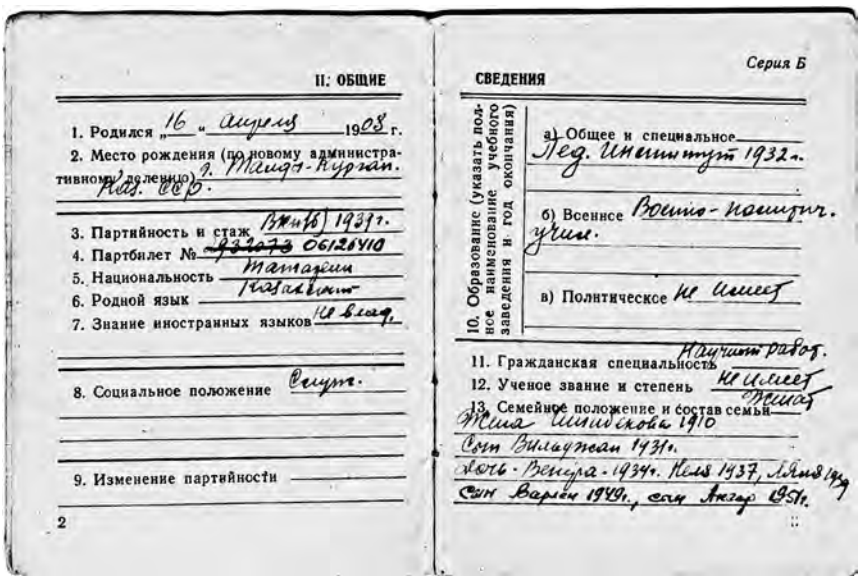
По-видимому, среди этих первых 124 студентов был и Мавлитдин Оспанович, т. к. его военный билет свидетельствует о том, что в 1932 г. он окончил педагогический институт. И, очевидно, был среди лучших студентов, т. к. к концу 1933 года уже

имел «*три года педстажа в ВУЗах*», т. е. уже работал преподавателем в собственном институте (других в Алма-Ате ещё не было) за два года до его окончания.

20 октября 1933 года Совнарком СССР принял Постановление № 2293 «О подготовке кадров для Казахстана», в котором было зафиксировано решение об организации в городе Алма-Ате (на базе кафедр КазПИ) Казахского государственного университета (КазГУ). Датой же его официального открытия принято считать 15 января 1934 года, когда был подписан приказ о профессорско-преподавательском составе (5 профессоров и 10 доцентов) и о зачислении первых 54 студентов на два факультета — физико-математический и биологический, на которых работало 25 преподавателей. Тогда же КазГУ было присвоено имя С. М. Кирова.

Размещались первоначально КазПИ и КазГУ в близко расположенных зданиях бывших мужской и женской гимназий.

Обратим внимание, что на приведённых фотографиях на фронтонах зданий Дворца труда и университета название



II. ОБЩИЕ

1. Родился „16" апреля 1908 г.
2. Место рождения (по новому административному делению) г. Талды-Курган. Каз. ССР.
3. Партийность и стаж Внп(б) 1931 г.
4. Партбилет № ~~931073~~ 06126410
5. Национальность Татарка
6. Родной язык Татарский
7. Знание иностранных языков Не владею.
8. Социальное положение Служ.
9. Изменение партийности
2

Серия Б

СВЕДЕНИЯ

10. Образование (указать полное наименование учебного заведения и год окончания)
а) Общее и специальное Пед. Институт 1932 г.
б) Военное Военно-политич. учил.
в) Политическое Не имеет
11. Гражданская специальность Не имеет работ.
12. Ученое звание и степень Не имеет
13. Семейное положение и состав семьи Замуж
Тетя Шишкова 1910
Сын Владислав 1931 г.
Мать - Вендра - 1934 г. Умер 1937, Умер 1939
Сын Вадим 1940 г., сын Анатолий 1951 г.

Из военного билета

СВЕДЕНИЯ О РАБОТЕ

№ записи	Дата: Год	Месяц	Число	Сведения о приеме на работу, перемещениях по работе и увольнении (с указанием причин)	На основании чего внесена запись (документ, его дата и номер)
1	2			3	4
1.				Общий стаж работы по найму до поступления в Каз. Гос. Универс. 3 года три года, педстаж в ВУЗах.	[illegible] документами 3 года
2.	1934	I	23.	Зачислен штатным ассистентом Каз. Гос. Университета	Приказ №11 от 23/I 34 г.
3.	1935	X	1	Переведен на кафедру математики должность доцента	Пр. №131 от 1/X 35 г.
4.	1942	VI	25	Освобожден от работы в связи с призывом в РККА	Приказ Каз… №287 от 25.VI.1942 г.

Первые записи в трудовой книжке М. О. Амирбаева

учреждения на казахском языке дано, соответственно, в латинской и в арабской графике, что наглядно демонстрирует равноправное хождение тогда обоих вариантов и объясняет, почему Мавлитдину Оспановичу приходилось переводить учебники в обеих версиях.

Первая запись в трудовой книжке Мавлитдина Оспановича гласит, что 23 января 1934 г. он был «зачислен штатным ассистентом Каз. Гос. Университета». То есть через восемь дней после подписания приказа о профессорско-преподавательском составе (5 профессоров и 10 доцентов) и о зачислении первых 54 студентов, или через восемь дней после официальной даты открытия КазГУ.

Но перед этой записью есть другая: «*Общий стаж работы по найму до поступления в Каз. Гос. Универс. 3 года, три года, педстаж в ВУЗах*». То есть до этого он проработал три года «*в ВУЗах*», очевидно, в КазПИ, других тогда в Алма-Ате не было.

Следовательно, педагогический стаж Мавлитдина Оспановича начался с 1930 года и закончился (также согласно трудовой

книжке) 26 августа 1975 г. Всего 45 лет с 4-летним перерывом на войну с 25.07.1942 по 21.02.1946 гг.

В 1942 г. Мавлитдин Оспанович добровольно пошёл на фронт (отказался от брони, представленной ему как преподавателю вуза). Тогда в семье было уже четверо детей: старший сын Вильжан 11 лет и три дочери 8, 5 и 2,5 лет. Ашраф Ризаевне в эти трудные годы удалось сохранить и вырастить детей здоровыми.

Участник ВОВ Маулен[3] (Мавлитдин) Оспанович Амирбаев

Воевал Мавлитдин Оспанович на Ленинградском и Прибалтийском фронтах в артиллерийском гвардейском миномётном полку, дошёл до Берлина и участвовал в войне с Японией.

За мужество и отвагу в боях с фашистами награждён орденами «Красная Звезда» и «Отечественной войны 2-й степени», медалью «За оборону Ленинграда» и другими наградами. Домой Мавлитдин Оспанович вернулся в ноябре 1945 года.

После войны Мавлитдин Оспанович продолжил преподавание высшей математики в КазГУ и КазПИ.

За свои труды он получил учёную степень кандидата физико-математических наук, звание доцента и награды — «Знак Почёта», «Заслуженный учитель Казахстана».

---

[3] В кругу родных и друзей его называли Маулен.

СЕКРЕТНО
экз. № 2

ПРИКАЗ

КОМАНДУЮЩЕГО АРТИЛЛЕРИЕЙ КРАСНОЙ АРМИИ

№ 015/н.

" 3 " августа 1945г. гор.Москва.

От имени Президиума Верховного Совета Союза ССР за образцовое выполнение боевых заданий Командования на фронте борьбы с немецкими захватчиками и проявленные при этом доблесть и мужество -НАГРАДАЮ:

ОРДЕНОМ КРАСНОГО ЗНАМЕНИ.

1.Гвардии капитана БРЫНЦЕВА Александра Степановича-помощника начальника штаба 320 гвардейского минометного Красносельского Краснознаменного полка.

ОРДЕНОМ ОТЕЧЕСТВЕННОЙ ВОЙНЫ 1-СТЕПЕНИ.

1.Гвардии майора ОСИПОВА Александра Семеновича-заместителя командира 64 гвардейского минометного Свирского Краснознаменного полка по строевой части.

ОРДЕНОМ ОТЕЧЕСТВЕННОЙ ВОЙНЫ 2-СТЕПЕНИ.

1.Гвардии майора АНДРЕЕВА Ивана Ивановича-заместителя командира 3 дивизиона 320 гвардейского минометного Красносельского Краснознаменного полка по политчасти.

2.Гвардии капитана ЗОРИЧ Якова Николаевича-командира батареи 53 гвардейского минометного полка.

3.Гвардии капитана КОЧЕТКОВА Василия Михайловича-начальника штаба дивизиона 52 гвардейского минометного полка.

4.Гвардии капитана ПИЛИПЕНКО Михаила Дмитриевича-офицера разведки 52 гвардейского минометного полка.

ОРДЕНОМ КРАСНОЙ ЗВЕЗДЫ.

1.Гвардии красноармейца АПАШИНА Ивана Осиповича-красноармейца 2 учебной бригады гвардейских минометных частей.

2.Гвардии старшего лейтенанта АМИРБАЕВА Мавлитдина Оспановича-парторга 3 дивизиона 320 гвардейского минометного Красносельского Краснознаменного полка.

Из приказа о награждении орденом Красной Звезды

НАГРАДНОЙ ЛИСТ

Фамилия, имя и отчество – АМИРБАЕВ Мавлитдин Оспанович

Воинское звание – гвардии старший лейтенант.

Должность, часть – Парторг 3-го дивизиона 320 Гвардейского минометного краснознаменного полка.

ПРЕДСТАВЛЯЕТСЯ К ОРДЕНУ "ОТЕЧЕСТВЕННАЯ ВОЙНА" II-й степени

1. Год рождения – 1903 г. 2. Национальность – татарин.
2. С какого года состоит в Красной Армии – с 1942 г.
3. Партийность – член ВКП(б) с 1939 г.
4. Участие в боях – Отечественная война с 1942 г. на Ленинградском 3-й Прибалтийском и 2-м Прибалтийском фронтах.
5. Имеет ли ранения и контузии – Легкое ранение в 1943 г. на Ленинградском фронте.
6. Чем ранее награжден – Медаль "За оборону Ленинграда".
7. Каким РВК призван – Сталинский РВК г.Алма-Ата.
8. Постоянный домашний адрес –

I. КРАТКОЕ, КОНКРЕТНОЕ ИЗЛОЖЕНИЕ ЛИЧНОГО БОЕВОГО ПОДВИГА ИЛИ ЗАСЛУГ.

АМИРБАЕВ Мавлитдин Оспанович работая парторгом дивизиона непосредственно в боевых условиях приобрел опыт руководящей работы.

Работу первичной партийной организации направляет на помощь командирам. У коммунистов воспитывает большевистскую принципиальность и любовь к социалистической родине. В боях с немецкими захватчиками показывал примеры мужества и храбрости, не щадя личной опасности неоднократно выезжал с орудийными расчетами на стрельбу прямой наводкой.

В районе г.Тарту 24 августа 1944 года выполняя приказ командира полка вместе с двумя орудийными расчетами выехал на стрельбу прямой наводкой по контратакующему противнику. Под сильным обстрелом т.АМИРБАЕВ личным примером мужества и храбрости воодушевлял гвардейцев орудийных расчетов на героические подвиги. Орудия во время выехали на огневые позиции и своевременными залпами отбили контратакующего противника.

ВЫВОД: За проявленные личные боевые качества – храбрость и мужество в бою при выполнении приказа командира т.АМИРБАЕВ М.О. достоин правительственной награды орденом "Отечественная война" II степени.

КОМАНДИР 320 ГВАРДЕЙСКОГО МИНОМЕТНОГО КРАСНОЗНАМЕННОГО ПОЛКА
ГВАРДИИ подполковник /ЗЫРИН/

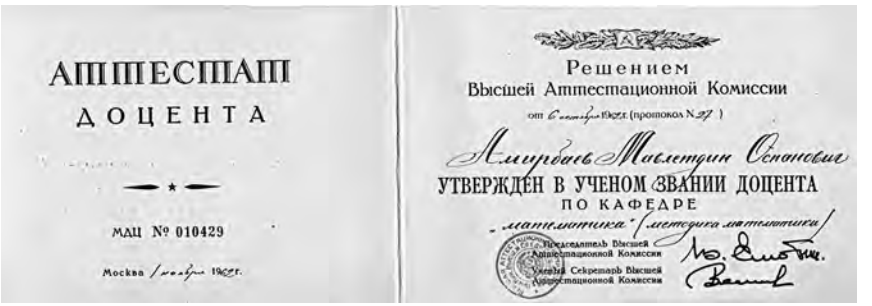
"14" июня 1945 года.

Орден Красной Звезды — наградной лист

Удостоверение к ордену Отечественной войны М. О. Амирбаева

Удостоверение М. О. Амирбаева к медали «За оборону Ленинграда»

Мавлитдин Оспанович (5-й справа в первом ряду)
в группе выпускников КазПИ



АТТЕСТАТ
ДОЦЕНТА

МДЦ № 010429

Москва / ноября 19 г.

Решением
Высшей Аттестационной Комиссии
от 6 октября 19 г. (протокол № 27)

Амирбаев Мавлетдин Оспанович
УТВЕРЖДЁН В УЧЕНОМ ЗВАНИИ ДОЦЕНТА
ПО КАФЕДРЕ
математика / методика математики

Председатель Высшей Аттестационной Комиссии

Ученый Секретарь Высшей Аттестационной Комиссии

Аттестат доцента М. О. Амирбаева

Завершим рассказ об отце Вильжана Мавлютиновича статьёй, опубликованной в 2002 г. в спецвыпуске журнала КазПИ, посвящённого ветеранам Великой Отечественной войны.

АМИРБАЕВ
Мавлитдин Оспанович

Родился 16 апреля 1908 г. в г. Талды-Курган.
В 1942 г. был призван в Красную Армию.
С 1942 по 1943 гг. участвовал в боях на Ленинградском фронте, перенес все тяжести Ленинградской обороны, шагая по бездорожью и болотам родной земли. Но задача была выполнена: части Советской Армии прорвали Ленинградскую блокаду. С 1944 по май 1945 гг. воевал в частях 2-го, затем 3-го Прибалтийских фронтов Отечественной войны. С 1945 по 1946 гг. находился в резерве политуправления МВО. Демобилизован в запас в 1946 г. И в том же году принят на работу в КазГУ им. С.М. Кирова на должность старшего преподавателя. В 1947 г. переходит на работу в КазГосЖенПИ. Здесь он защищает кандидатскую диссертацию по математическим уравнениям, получает звание доцента кафедры математики. В 1975 г. вышел на пенсию.
За заслуги перед Родиной Мавлитдин Оспанович награжден орденами "Красной звезды" и "Знак Почета", медалями "За оборону Ленинграда", "За победу над Германией", "За доблестный труд", а также многими юбилейными медалями в честь исторических дат Советской армии. Награжден Почетным знаком "Отличник народного просвещения КазССР" и медалью "Ветеран труда".
Амирбаев М.О. является одним из основателей женского педагогического института. Он стоял у истоков его формирования и развития, многое сделал для того, чтобы подготовить высококвалифицированных математиков среди девушек-казашек. Писал научные статьи и методические пособия по вопросам математики, которые не потеряли своего значения и по сей день.

Статья о М. О. Амирбаеве

Детство и юность

В 1938 г. Вильжан пошёл в 1-й класс новой тогда школы № 25, построенной в 1937-м. Она располагалась на углу улиц Калинина (ныне Кабанбай батыра) и Дзержинского (ныне Наурызбай батыра). Напротив через ул. Калинина находилось здание КГБ,

а через ул. Фрунзе — милицейский стадион «Динамо». Неудивительно, что в таком окружении школа первоначально была названа именем Ежова, однако после ареста опального руководителя НКВД она получила имя Феликса Эдмундовича Дзержинского и носила его вплоть до 1990-х годов. Рядом со школой (и с КГБ) стоял памятник Ф. Э. Дзержинскому.

Тогда это была одна из элитных школ с очень высоким уровнем обучения.

Школа № 25 в Алма-Ате

Школу Вильжан окончил с золотой медалью.

С детских лет он имел хорошую физическую подготовку, занимался спортом и туризмом в примыкающих к Алма-Ате горах Заилийского Ала-Тау.

В том же 1949 г. Вильжан поступил в КазГУ им. Кирова на физико-математический факультет.

Вильжан после выпускных экзаменов в школе

В КазГУ была и военная кафедра, в результате обучения на которой после завершающих сборов в войсковых частях молодые люди получали звание «младший лейтенант» Советской армии.

Летом 1954 г. Вильжан закончил КазГУ с красным (с оценками «отлично») дипломом, получив первое научное звание — младший научный сотрудник. На общей фотографии выпуска Вильжан Мавлютинович Амербаев левый в верхнем ряду выпускников. А в центре четвёртого сверху ряда — его однокашник и друг на всю жизнь, активный участник подготовки настоящего сборника Иван Тимофеевич Пак.

На военных сборах. Третий стоящий справа Вильжан Амербаев, седьмой — его друг Иван Пак, 1953 г.

Диплом необычен для россиян — он на двух языках, т. к. в союзных республиках СССР было по два государственных языка — национальный и русский.

ДИПЛОМ

ҮЗДІК БЕЛГІМЕН

З № 006983

Осы диплом Амербаев Вильжсан Мавлютиновичке берілді, ол 1949 жылы Қазақтың С.М.Киров атындағы Мемлекеттік университетінің физико-математика факультеті, 1954 жылы осы аталған факультеттің толық курсын математика мамандығы бойынша бітіріп шықты.

Мемлекеттік емтихан комиссиясының 1954 жылғы 30 июньдегі қарары бойынша оған кіші ғылыми қызметкері Жоғарғы Оқу орынд. және орта мектептің жоғарғы кл. оқытуш. деген квалификация берілді.

Мемлекеттік емтиған комиссиясының председателі
Ректор (Директор) Секретарь

М. О.

Алматы қаласы 1/VII 1954 жыла

Тіркеу № 737

Нагрудный знак выдан

ДИПЛОМ

С ОТЛИЧИЕМ

З № 006983

Настоящий диплом выдан Амербаеву Вильжсану Мавлютиновичу в том, что он в 1949 году поступил в Казахский государственный университет им. С.М. Кирова на физико-математический факультет, и в 1954 году окончил полный курс названного факультета по специальности математика

Решением Государственной экзаменационной комиссии от 30 июня 1954 г. ему присвоена квалификация млад. научн. сотрудн., препод. ВУЗов и старшина класса С.Ш

Председатель Государственной экзаменационной комиссии
Ректор (директор)
Секретарь

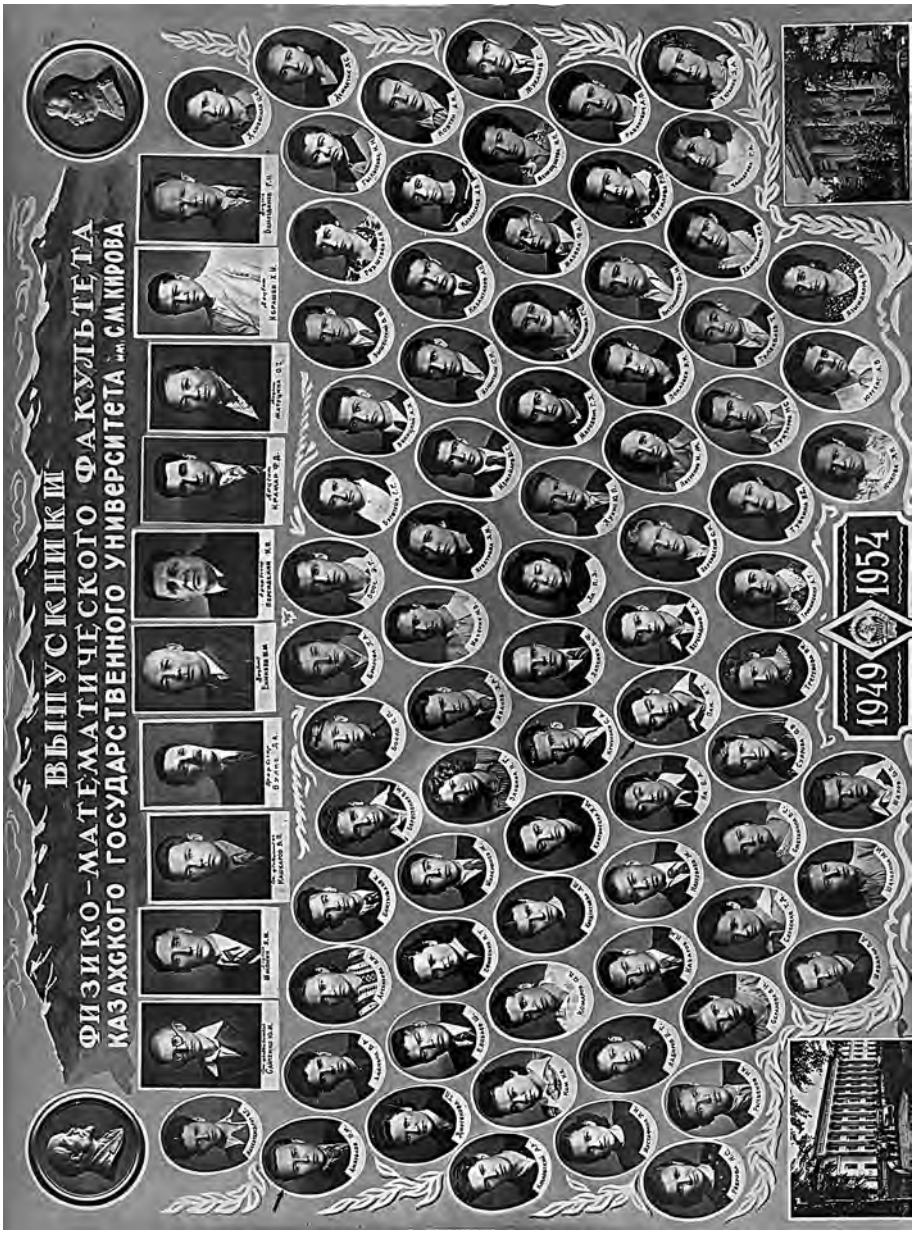
М. П.

Город Алма-Ата 1/VII 1954 г.

Регистрационный № 737

Типография им. В. М. Молотова. Гознак. 1953.

Диплом м.н.с. В. М. Амербаева



Выпускники КазГУ 1954 года

Работа

И сразу же, с 1.09.1954 г., Вильжан был зачислен на должность ассистента кафедры дифференциальных уравнений КазГУ, где проработал до 28.11.1956 г., до поступления в аспирантуру Математического института им. В. А. Стеклова в Москве.

СВЕДЕНИЯ О РАБОТЕ

№ записи	Дата: Год	Дата: Месяц	Дата: Число	Сведения о приеме на работу и увольнении	работу, перемещениях по (с указанием причин)	На основании чего внесена запись (документ, его дата и номер)
1	2				3	4
				Общего стажа работы до поступления нет.	Казгосуниверситет.	
1	1954	IX	1	Зачислен на ассистента кафедры дифференциальных	Ассистент. Должность кафедра дифференциальных уравнений.	Приказ № 755 от 14/IX-1954 г.
2	1956	XI	28	Освобожден в связи с поступлением в аспирантуру	Работал в Казгосуниверситете	Приказ № 185 от 21/11-1957 г.

Из трудовой книжки: 1954–1956 гг. — КазГУ

Уже в те времена у студентов был «третий семестр» — летне-осенний. Они активно в течение почти месяца участвовали в «битве за урожай» — так в СССР называлась уборка сельскохозяйственной продукции. В качестве руководителей со студентами посылали работников университета, обычно из молодёжи. В 1955 г. в «битве за урожай» активное участие принимал ассистент кафедры дифференциальных уравнений Вильжан Амербаев.

В 1955–1959 гг. Вильжан — аспирант Математического института им. В. А. Стеклова АН СССР (МИАН) в Москве.

Здесь молодой Вильжан остро прочувствовал, что его отличные оценки в КазГУ ни в коей мере не обеспечили уровня

знаний, требуемого в Москве. Четыре года обучения в аспирантуре под руководством ведущих математиков страны он использовал для углубления знаний по высшей математике. А диссертацию он защитил позже, защитил прекрасно.

Третий семестр на уборке хлопка, Пахта-Арал,
совхоз им. Коминтерна, 1955 г.

По окончании аспирантуры параллельно с подготовкой диссертации Вильжан Мавлютинович с 16.11.1959 по 27.12.1965 гг. работал в должностях младшего научного сотрудника, заведующего лабораторией машинной и вычислительной математики АН КазССР. Лаборатория была самостоятельной структурой при президиуме АН.

№ записи	Дата: Год	Дата: Месяц	Дата: Число	Сведения о приеме на работе и увольнении	работу, перемещениях по (с указанием причин)	На основании чего внесена запись (документ, его дата и номер)
1	2				3	4
				Академия	наук Каз. ССР	
3.	1959	XII	16	Зачислен на	должность млад	Пр. № 819 н
				шего научного сот	рудника лаборатории	21. XI. 59
				машино-вычислит	ной математики АН Каз ССР	
4	1962	XII	6	Назначен и.о	заведующего	Гос. ун. дер
				Лабораторией маш.	и вычислительной	Президиума № 148
				математики.		от 12/XII - 62 г.
5	1965	XII	27	Освобожден от	занимаемой	Гос. ун. бюро
				должности в связи	с переходом	Президиума
				на работу н/я 2014.		АН Каз. ССР
				Начальник отдела		№ 64 от 27/XII-65
				подготовки научных		
				АН Каз. ССР:	А. Арстанбеков.	

Из трудовой книжки: 1959–1965 гг. — АН КазССР

Решением

Совета Математ. ин-та им. В. А. Стеклова АН СССР

от 21 марта 1963 г. (протокол N 3)

Амербаеву Вильжану Маблютиновичу

ПРИСУЖДЕНА УЧЕНАЯ СТЕПЕНЬ КАНДИДАТА ФИЗИКО-МАТЕМАТИЧЕСКИХ НАУК

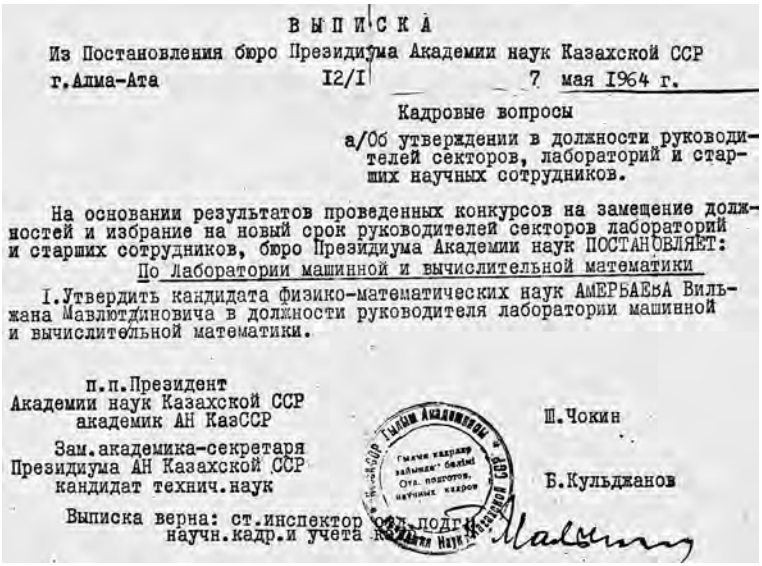
Председатель Совета

Ученый Секретарь Совета

Диплом кандидата физико-математических наук

В 1963 году Вильжан на учёном совете МИАН СССР защитил диссертацию кандидата физико-математических наук на тему «*Численные методы обращения интегрального преобразования Лапласа*», посвящённую разработке методов восстановления оригинала путём разложения его в ряд по ортогональным многочленам на конечном промежутке.

Исполняющим обязанности заведующего лабораторией В. М. Амербаев был назначен до защиты диссертации. А после защиты, поскольку лаборатория была непосредственно при президиуме академии, окончательное назначение было проведено специальным постановлением бюро президиума АН КазССР.



ВЫПИСКА

Из Постановления бюро Президиума Академии наук Казахской ССР

г.Алма-Ата 12/I 7 мая 1964 г.

Кадровые вопросы

а/Об утверждении в должности руководителей секторов, лабораторий и старших научных сотрудников.

На основании результатов проведенных конкурсов на замещение должностей и избрание на новый срок руководителей секторов лабораторий и старших сотрудников, бюро Президиума Академии наук ПОСТАНОВЛЯЕТ:

По лаборатории машинной и вычислительной математики

I.Утвердить кандидата физико-математических наук АМЕРБАЕВА Вильжана Мавлютдиновича в должности руководителя лаборатории машинной и вычислительной математики.

п.п.Президент
Академии наук Казахской ССР
академик АН КазССР Ш.Чокин

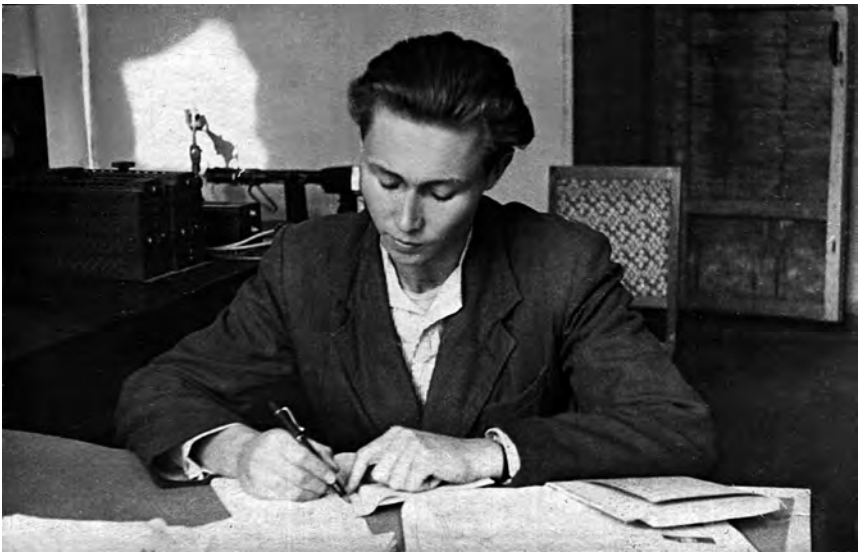
Зам.академика-секретаря
Президиума АН Казахской ССР
кандидат технич.наук Б.Кульджанов

Выписка верна: ст.инспектор отд.подготовки научн.кадр.и учета

Выписка о назначении завлабом

Параллельно с выполнением научной работы и с организацией работы лаборатории Вильжан активно занимался её развитием и оснащением. Так, в 1965 г. он проделал огромную работу по обоснованию необходимости новой тогда ЭВМ БЭСМ-6, добился решения о её выделении для лаборатории, организовывал её размещение и ввод в эксплуатацию.

Вильжан Мавлютинович активно участвовал в подготовке создания Института математики и механики АН КазССР, в определении основных научных направлений создаваемого института, которые были утверждены отделением математики Академии наук СССР. В частности, ему удалось обосновать направление по вычислительной математике и вычислительной технике.



На рабочем месте

Открытие Института математики и механики АН КазССР состоялось в сентябре 1965 г. на базе сектора математики и механики и лаборатории машинной и вычислительной математики.

Но в новом институте Вильжан Мавлютинович проработал всего четыре месяца.

Зеленоград, 1966–1972 гг.

В 1965 г. в Алма-Ату из Москвы (Зеленограда) приехали Давлет Исламович Юдицкий и Израиль Яковлевич Акушский (основатель и первый руководитель лаборатории машинной и вычислительной математики в Алма-Ате) и провели ряд научных семинаров по применению новой тогда системы счисления

остаточных классов (СОК). Вильжана Мавлютиновича весьма заинтересовала идея модулярной арифметики, он увидел в ней ряд перспективных уникальных возможностей, ночью провёл свои первые исследования и доложил о них на следующем семинаре. И этим весьма заинтересовал гостей, которые увидели в нём крайне необходимого им специалиста. Они предложили Вильжану Мавлютиновичу работу в Зеленограде, он принял предложение и с 6 января 1966 г. приступил к работе в качестве старшего научного сотрудника зеленоградского предприятия п/я 2014 инновационного Центра микроэлектроники (ЦМ) Министерства электронной промышленности СССР (МЭП). В коллективе Юдицкого он проработал более шести лет до приглашения его в 1972 г. в АН КазССР. Коллектив этот в результате переименований и реорганизаций претерпел изменения: предприятие п/я 2014 — НИИ физических проблем (НИИФП) — научно-технический комплекс (НТКС) в составе НИИФИ — специализированный вычислительный центр (СВЦ), что отразилось в трудовой книжке В. М. Амербаева.

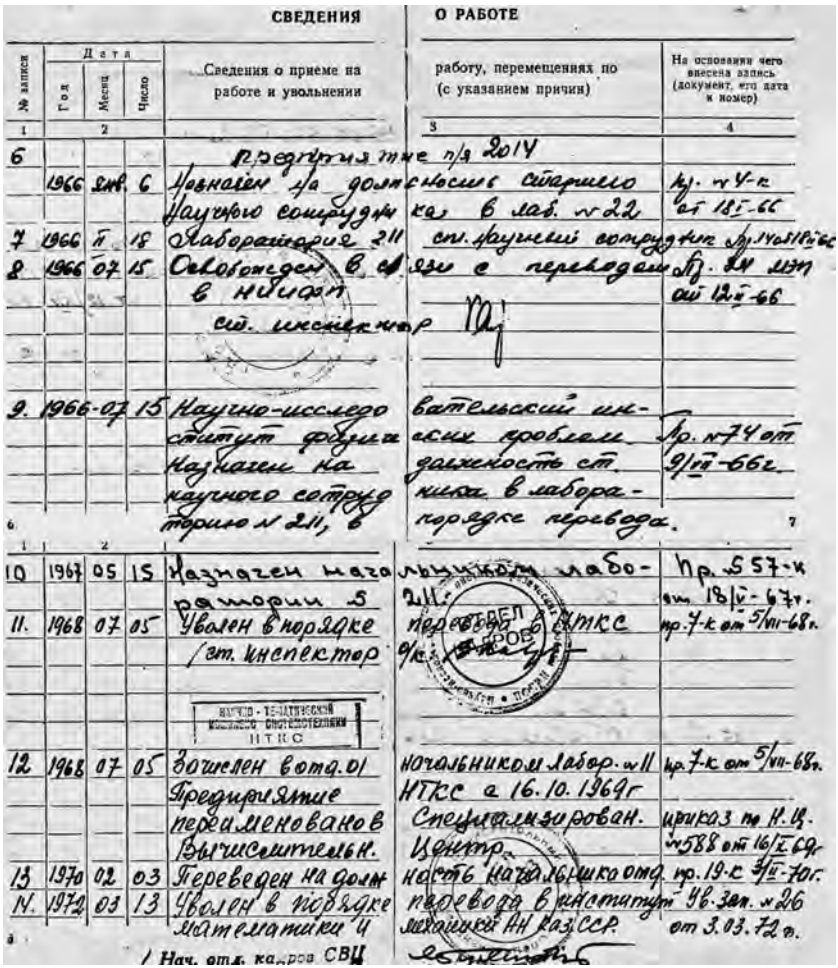
Здесь необходимо отметить, что за время жизни и работы в Зеленограде В. М. Амербаев никогда не терял творческих и дружеских связей с учёными АН КазССР и её Институтом математики и механики. Поэтому он был всегда в поле зрения академии наук, что привело к двум его возвращениям в Алма-Ату. Но об этом далее.

В первый приезд в Зеленоград В. М. Амербаев принял активное участие в разработке высокопроизводительной модулярной супер-ЭВМ для системы противоракетной обороны (ПРО) МКСК «Аргунь» на этапах эскизного (проект «Алмаз») и технического (проект 5Э53) проектирования. Основной его задачей было совершенствование алгоритмов выполнения операций в тогда ещё новой модулярной арифметике в целях повышения производительности, точности и надёжности ЭВМ и оптимизации их практической схемотехнической реализуемости. По успешном окончании этой работы Вильжан Мавлютинович занимался дальнейшим развитием модулярной арифметики применительно к перспективному тогда проекту

ЭВМ IV — ЭВМ 4-го поколения, в т. ч. реализацией табличной модулярной арифметики.

В середине 1967 г. Вильжан Мавлютинович был утверждён в учёном звании старшего научного сотрудника.

В 1970 г. В. М. Амербаев был награждён медалью СССР «*За доблестный труд. В ознаменование 100-летия со дня рождения Владимира Ильича Ленина*».



СВЕДЕНИЯ О РАБОТЕ

№ записи	Дата: Года	Месяц	Число	Сведения о приеме на работе и увольнении	работу, перемещениях по (с указанием причин)	На основании чего внесена запись (документ, его дата и номер)
1	2				3	4
6				предприятие п/я 2014		
	1966	янв.	6	Уволен п/я должность старшего		ку. №4-к
				научного сотрудника в лаб. №22		от 18-I-66
7	1966	п	18	Лаборатория 211	ст. научный сотрудник	ку №40518-66
8	1966	07	15	Освобожден в связи с переводом		ку. ВЧ 3377
				в НИИФП		от 12-I-66
				ст. инспектор		
9.	1966	07	15	Научно-исследо	вательский ин-	
				ститут физиче	ских проблем	пр. №74 от
				Назначен на	должность ст.	9/II-66г.
				научного сотруд	ника в лабора-	
				ник лаборатории №211, в	порядке перевода.	
6						7
1	2					
10	1967	05	15	Назначен нача	льником лабо-	пр. 557-к
				ратории 5	211.	от 18/V-67г.
11.	1968	07	05	Уволен в порядке	переведен в НТКС	пр. 7-к от 5/VII-68г.
				/ст. инспектор		
				НАУЧНО-ТЕХНИЧЕСКИЙ КОМПЛЕКС СПЕЦТЕХНОЛОГИЙ НТКС		
12	1968	07	05	Зачислен вотд. 01	начальником лабор. №11	пр. 7-к от 5/VII-68г.
				Предприятие	НТКС с 16.10.1969г	
				переименовано в	Специализирован.	приказ по Н.Ц.
				Вычислительный	Центр	№588 от 16/X-69г.
13	1970	02	03	Переведен на долж	ность начальника отд.	пр. 19-к 3/II-70г.
IV.	1972	03	13	Уволен в порядке	перевода в институт	ув. зап. №26
				математики и	механики АН Каз. ССР	от 3.03.72 г.
				/ Нач. отд. кадров СВЦ		

Из трудовой книжки: 1966–1972 гг. — НИИФП—СВЦ

Решением
Высшей Аттестационной Комиссии
от 15 июля 1967 г. (протокол N 45/VI)
Амербаев Вильжан Мавлютинович
УТВЕРЖДЕН В УЧЕНОМ ЗВАНИИ
СТАРШЕГО НАУЧНОГО СОТРУДНИКА
ПО СПЕЦИАЛЬНОСТИ
„вычислительная математика"
Председатель Высшей Аттестационной Комиссии
Ученый Секретарь Высшей Аттестационной Комиссии

Аттестат старшего научного конструктора

„ЗА ДОБЛЕСТНЫЙ ТРУД. В ОЗНАМЕНОВАНИЕ 100-ЛЕТИЯ СО ДНЯ РОЖДЕНИЯ ВЛАДИМИРА ИЛЬИЧА ЛЕНИНА"
1870 – 1970
УДОСТОВЕРЕНИЕ
Амербаев
Вильжан
Мавлютинович
от имени ПРЕЗИДИУМА ВЕРХОВНОГО СОВЕТА СССР
НАГРАЖДЕН ЮБИЛЕЙНОЙ МЕДАЛЬЮ
„ЗА ДОБЛЕСТНЫЙ ТРУД.
В ОЗНАМЕНОВАНИЕ 100-ЛЕТИЯ
СО ДНЯ РОЖДЕНИЯ
ВЛАДИМИРА ИЛЬИЧА ЛЕНИНА"
М. П.
1 апреля 1970 года.

Медаль «За доблестный труд»

Результаты работ В. М. Амербаева также нашли отражение в публикациях статей, выступлениях на научных конференциях и в монографиях, а также в его докторской диссертации на тему «*Вычисления в кольце главных идеалов и их приложения в вычислительной технике*», которую он защитил в 1971 г. на учёном совете зеленоградского НПО «Элас».


Решением
Высшей Аттестационной Комиссии
от 11 июня 1971 г. (протокол N 24/с)
Амербаеву Вильжану Мавлютиновичу
ПРИСУЖДЕНА УЧЕНАЯ СТЕПЕНЬ ДОКТОРА
ТЕХНИЧЕСКИХ НАУК
Председатель Высшей Аттестационной Комиссии
Ученый Секретарь Высшей Аттестационной Комиссии

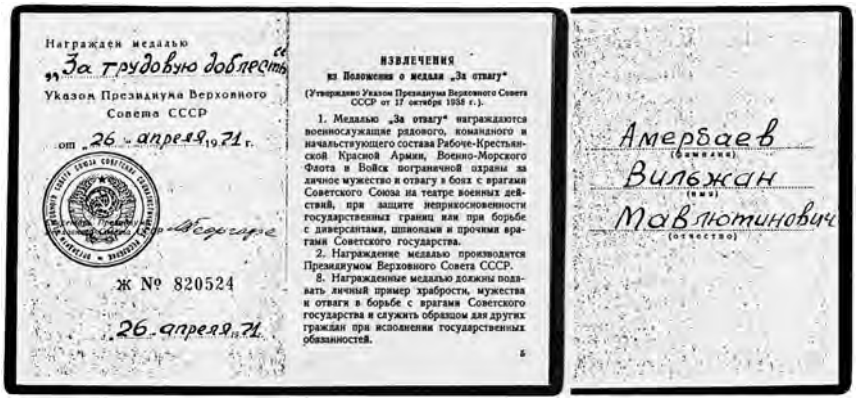
Диплом доктора технических наук

Проект 5Э53 был завершён успешно и в срок.

Для Вильжана Мавлютиновича это событие было отмечено награждением медалью СССР «За трудовую доблесть».

Но, к сожалению, Минрадиопром прекратил работы по проекту МКСК «Аргунь», а вместе с ним и работы по освоению 5Э53 в производстве. Но это другая история.

В этих условиях в начале 1972 г. Вильжан Мавлютинович получил предложение АН КазССР занять должность заместителя директора Института математики и механики АН КазССР, к созданию которого он ранее имел непосредственное отношение.



Награжден медалью
„За трудовую доблесть"
Указом Президиума Верховного Совета СССР
от 26 апреля 1971 г.
Ж № 820524
26 апреля 1971

ИЗВЛЕЧЕНИЯ
из Положения о медали „За отвагу"
(Утверждено Указом Президиума Верховного Совета СССР от 17 октября 1938 г.).

1. Медалью „За отвагу" награждаются военнослужащие рядового, командного и начальствующего состава Рабоче-Крестьянской Красной Армии, Военно-Морского Флота и Войск пограничной охраны за личное мужество и отвагу в боях с врагами Советского Союза на театре военных действий, при защите неприкосновенности государственных границ или при борьбе с диверсантами, шпионами и прочими врагами Советского государства.

2. Награждение медалью производится Президиумом Верховного Совета СССР.

8. Награжденные медалью должны подавать личный пример храбрости, мужества и отваги в борьбе с врагами Советского государства и служить образцом для других граждан при исполнении государственных обязанностей.

5

Амербаев
(фамилия)
Вильжан
(имя)
Мавлютинович
(отчество)

Награждение медалью «За трудовую доблесть»

Здесь уместно отметить редкую черту характера Вильжана Мавлютиновича. Главным интересом его жизни была высшая математика с ориентацией на вычислительную технику. Ею он готов был заниматься круглосуточно. Для него это были и работа, и отдых, и хобби. Он всегда стремился быть там, где есть сложная математическая проблема, и с энтузиазмом брался за её решение. Он особо ценил, если рядом были такие же одержимые энтузиасты — люди честные, добропорядочные, всецело отдающие себя общему делу, особенно молодые. И тогда он отдавал им всего себя, весь свой опыт, знания, время. Но если задача реально или в глазах руководителей теряла свою актуальность, если возникали не зависящие от него препятствия к её решению, он терял к ней интерес и искал другую интересную задачу, искал новое место, где имелась такая задача. Интриг, «подковёрной» борьбы, непорядочности и людей, их практикующих, он не терпел и всячески избегал. Именно поэтому он иногда менял место своей работы «по собственному желанию».

Как вспоминает И. Т. Пак, «*к началу 1970-х годов в Институте математики и механики все ещё не было ни одного специалиста по вычислительной математике и вычислительной технике с докторской степенью, а Институт остро нуждался в таком*

специалисте. Вильжан Мавлютинович уже был доктором наук. На президиуме Академии наук КазССР было предложено вернуть его. И в 1971 году он был приглашён в Алма-Ату на должность заместителя директора Института математики и механики. Уже в следующем 1972 году Вильжан Мавлютинович избирается членом-корреспондентом АН КазССР.

Возвращение Вильжана Мавлютиновича сыграло важную роль в развитии вычислительной математики в Казахстане. Кроме того, получило толчок важное направление создания различных информационных систем, а также теория кодирования».

Алма-Ата, 1972–1977 гг.

13 марта 1972 г. В. М. Амербаев на время до прохождения конкурса был назначен и. о. завотделом вычислительной математики института. Конкурс оказался не быстрым, но всё же 18 августа он стал заместителем директора по научной работе Института математики и механики АН КазССР. В этой должности он проработал четыре с половиной года.

ЖҰМЫСЫ ТУРАЛЫ МӘЛІМЕТТЕР

Жазылу №	Уақыты: Жылы	Айы	Күні	Жұмысқа алынғаны, жұмыс тарылғаны туралы мәліметтер	женінде ауысқаны және шы- (себептері көрсетілсін)	Неге сүйеніп жазылды (документ, оның берілген уақыты мен номері)
1	2				3	4
15	1972	03	14	Институт м механики Назначен на и.о. зав. отде ной математи техники, в до прохождени	математики АН Каз ССР должность зом вычислитель и вычислительной норяке перевода по конкурсу	Приказ №37 §1 от 24/III-72г.
16	1972	08	18	Назначен зам. ик-та мате ханики АН	директора по наук. работе матики и ме- Каз ССР от занимае-	Пр №119 §1 от 21/VIII-72г
17	1977	09	01	Освобожден моей должнос с прохожден ер на долж кафедрой	в связи Конкур- ав	Пр №16 от 31/I 1977г.
20				Ст. инспектор		21

Из трудовой книжки: 1972–1977 гг. — ИММ АН КазССР

В том же 1972 г. В. М. Амербаев был избран членом-корреспондентом АН КазССР.

В качестве заместителя директора он с головой окунулся в улучшение и активизацию научно-организационной работы в институте, в первую очередь по мобилизации научных сил и привлечению молодых специалистов к выполнению приоритетных для Казахстана научно-исследовательских работ. В этот период открываются новые лаборатории: теории кодирования, методов оптимизации, больших систем, комбинаторных методов теории информации...

Несмотря на активную административно-организационную деятельность, Вильжан Мавлютинович всегда оставался профессиональным математиком. В частности, им успешно проводились исследования по применению модулярной арифметики в криптографии, в алгоритмах шифрования в целях повышения скорости криптографического преобразования путём распараллеливания процедур арифметических операций. Исследования привели к разработке новой концепции построения интромодулярных вычислительных систем.

Но эту плодотворную деятельность прервали события, от него не зависящие. В начале 1977 г. по семейным обстоятельствам Вильжан Мавлютинович с супругой вернулись в Зеленоград.

Москва, МИИГА, 1977–1979 гг.

Но в Зеленограде произошли крупные реорганизации и смена тематики, интересных для В. М. Амербаева математических задач не было. Пришлось переключиться на преподавательскую работу в вузе.

Первым местом работы был Московский институт инженеров гражданской авиации (МИИГА) с прохождением конкурса на должность заведующего кафедрой электронных вычислительных машин.

Всё было ново, всё было интересно. Особенно радовало его большое количество молодёжи. В 1977 г. Вильжан Мавлютинович получил звание профессора по кафедре вычислительной математики.

ЖҰМЫСЫ ТУРАЛЫ МӘЛІМЕТТЕР

Жазылу №	Уақыты: Жылы	Уақыты: Айы	Жұмыска алынғаны, жұмыс орындарын ауыстыруы, оларды тоқтатуы	жөнінде ауысқаны және шығу (себептері көрсетілсін)	Негіз сүйекін жазылды (документ, оның берілген уақыты мен нөмері)
1	2			3	4
18	1977	02	01 Зачислен на кафедрой счислительные	должность зав. электронные вы- машины, как	пр. 20/л от 4.02.77г.
19.	1979	09	01 Уволен по с	о конкурсу. общ. Основному	пр. №60/л 25/VI-79г.
			ст. шее	кто он бы-	

Из трудовой книжки: 1977–1979 гг. — МИИГА

В. М. Амербаев в форме высшего начальствующего состава 12-й категории МГА СССР


Решением
Высшей аттестационной комиссии
при Совете Министров СССР
от 6 мая 1977 г. (протокол № 18)
Амербаеву Вильжану Мавлютинов
присвоено ученое звание
ПРОФЕССОРА
по специальности
"Вычислительная математика"
Председатель
Высшей аттестационной комиссии
Ученый секретарь
Высшей аттестационной комиссии

Аттестат профессора

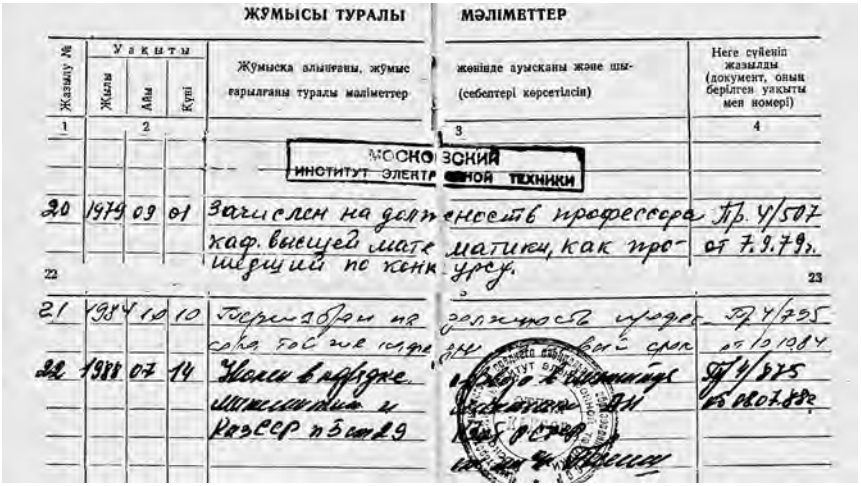
Но вскоре он заскучал. Ему не хватало реальных научных задач для исследований, соответствующих его интересам — в МИИГА таких не было. Какое-то время он продолжал самостоятельно работать в ранее начатых направлениях, но имеющего серьёзную практику решения реальных практических задач при разработке ЭВМ учёного абстрактные исследования не удовлетворяли. И ездить из Зеленограда в МИИГА (три вида транспорта, 1,5 часа в один конец) было уже тяжело. В результате Вильжан Мавлютинович решил перейти в зеленоградский МИЭТ. И близко, и реальные задачи легче найти на зеленоградских предприятиях.

В середине 1979 г. он подал заявление в МИЭТ, чтобы участвовать в конкурсе на замещение должности профессора.

Зеленоград, МИЭТ, 1979–2002 гг.

Вильжан Мавлютинович прошёл конкурс и 1 сентября 1979 г. начал работу в качестве профессора кафедры вычислительной

математики в Московском институте электронной техники (МИЭТ, Зеленоград).


ЖҰМЫСЫ ТУРАЛЫ МӘЛІМЕТТЕР

Жазылу №	Уақыты: Жылы	Айы	Күні	Жұмысқа алынғаны, жұмыс ғарылғаны туралы мәліметтер	жөнінде ауысқаны және шы- (себептері көрсетілсін)	Неге сүйеніп жазылды (документ, оның берілген уақыты мен номері)
1	2				3	4
				МОСКОВСКИЙ ИНСТИТУТ ЭЛЕКТРОННОЙ ТЕХНИКИ		
20	1979	09	01	Зачислен на должность профессора каф. высшей математики, как прошедший по конкурсу.		Пр. 4/507 от 7.9.79 г.
21	1984	10	10	Переведен на должность профессора каф. высшей математики		Пр 4/735 от 10.10.84
22	1988	07	14	Уволен в порядке перевода в Институт математики АН КазССР п 5 ст 29		Пр 4/575 от 08.07.88 г.

Из трудовой книжки: 1979–1988 гг. — МИЭТ

23 мая 1983 г. скоропостижно, находясь в командировке на Сары-Шаганском полигоне в Прибалхашье, на 53-м году жизни скончался Давлет Исламович Юдицкий. Вильжан Мавлютинович очень тяжело переживал смерть близкого друга. Именно тогда у него случился первый сердечный приступ.

Впоследствии Вильжан Мавлютинович часто возвращался к Давлету Исламовичу, вспоминая в соответствующей ситуации его слова или поступки. Не забывали его и многие СВЦ-шники, около 30 лет они встречались в дни его юбилеев или годовщин кончины.

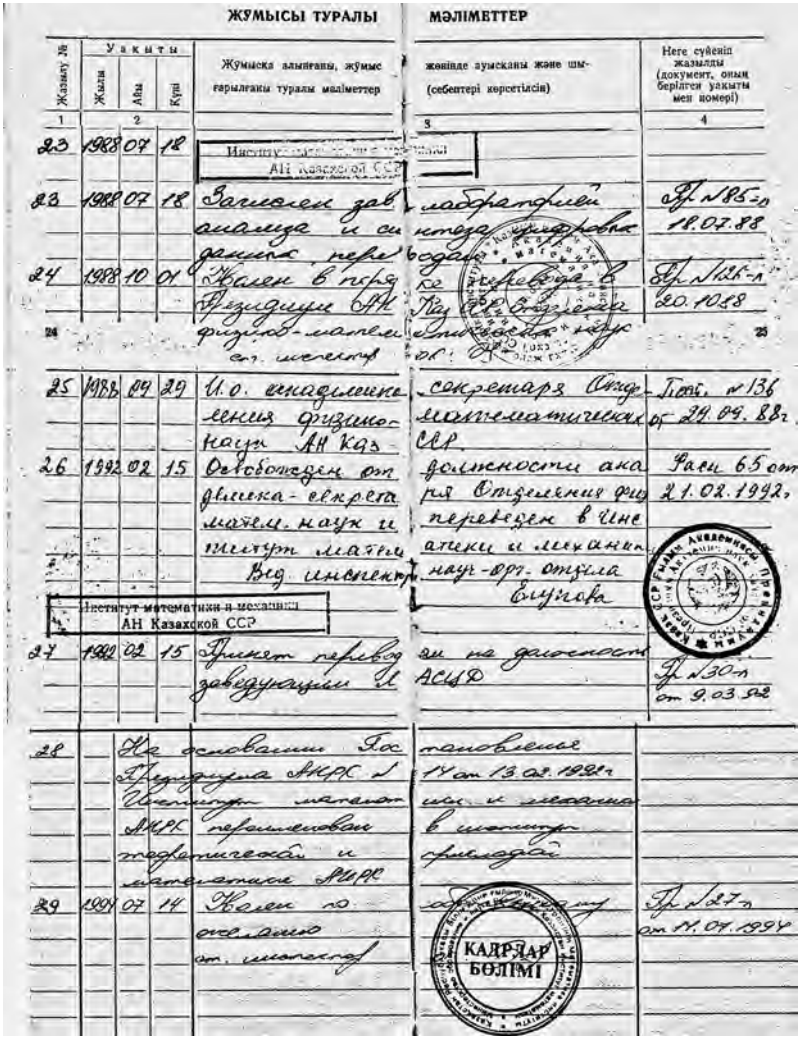
В МИЭТе с некоторыми перемещениями при реорганизациях института Вильжан Мавлютинович проработал до июля 1988 г. — до приглашения в Национальную академию наук Республики Казахстан (НАН РК) — так в независимом Казахстане называется бывшая АН КазССР.

20-летие памяти Д. И. Юдицкого, 25.05.2003 г.
В. М. Амербаев отмечен стрелкой

20-летие памяти Д. И. Юдицкого, 5.05.2003 г.
В. М. Амербаев стоит 4-й слева

Алма-Ата, 1988–1994 гг.

Весной 1988 г. в АН КазССР освободилось место академика-секретаря отделения физико-математических наук. Президентом академии в это время был У. М. Султангазин — математик,



ЖҰМЫСЫ ТУРАЛЫ МӘЛІМЕТТЕР

Жазылу №	Уақыты: Жылы	Айы	Күні	Жұмысқа алынғаны, жұмыс тағайындалғаны туралы мәліметтер	жөнінде алынғаны және шығ- (себептері көрсетілсін)	Негіз сүйеніп жазылды (документ, оның берілген уақыты мен номері)
1	2				3	4
23	1988	07	18	Институт [illegible] АН Казахской ССР		
23	1988	07	18	Зачислен зав. аспирантурой отдела [illegible] переводом		Пр. №85-л 18.07.88
24	1988	10	01	Избран в порядке перевода в Президиум АН Каз ССР отделения физико-математ. наук		Пр. №126-л 20.10.88
24						25
25	1988	09	29	И.о. академика-секретаря Отделения физико-математических наук АН Каз ССР		Прот. №136 от 29.09.88 г.
26	1992	02	15	Освобожден от должности академика-секретаря Отделения физико-математ. наук и назначен ст. науч. сотр. Института математики	переведен в Институт математики и механики науч.-орг. отдела Бугрова	Расп. 65 от 21.02.1992 г.
				Вед. инспектор		
				Институт математики и механики АН Казахской ССР		
27	1992	02	15	Принят переводом заведующим [illegible]	[illegible] на должность АСиД	Пр. №30-л от 9.03.92
28				На основании Постановления Президиума АН РК и Института математики АН РК переименован в Институт информатики и математики АН РК	постановления 14 от 13.03.1992 г. математики и механики в Институт информатики	
29	1994	07	14	Уволен по собственному желанию ст. инженер		Пр. №27-л от 11.07.1994

КАДРЛАР БӨЛІМІ

Из трудовой книжки: 1988–1994 гг. — Алма-Ата

бывший директор института математики и механики, хорошо знавший Амербаева. Он и пригласил 57-летнего Вильжана Мавлютиновича на освободившееся место. Глубоко уважая академика У. М. Султангазина, он согласился.

После прохождения положенных процедур Вильжан Мавлютинович был избран действительным членом АН КазССР и назначен академиком-секретарём отделения и членом президиума АН КазССР.

Отделение физико-математических наук, соединяющее в себе и математиков, и физиков, и астрофизиков, имело большие научные достижения, прекрасные кадры, проводило крупные международные конференции и совещания. Здесь Вильжан Мавлютинович был на своём месте.

Удостоверение академика АН КазССР

Удостоверение академика-секретаря ОФМН АН КазССР

За три с половиной года его работы академиком-секретарём отделение стало одним из ведущих подразделений академии наук

республики. В состав отделения входили ряд крупных институтов физико-математического направления: Институт ядерной физики, Физико-технический институт, Институт физики высоких энергий, Астрофизический институт им. В. Г. Фесенкова, Институт ионосферы, а также пять новых институтов, образованных на базе Института математики и механики: Институт теоретической и прикладной математики, Институт механики, Институт проблем информатики и управления, Институт космических исследований, Институт прикладной математики (в Караганде). Институт физики высоких энергий разделился на Институт физико-технический и Институт физики высоких энергий.

В этих преобразованиях и определении научных направлений новых институтов существенная роль принадлежала академику-секретарю отделения Вильжану Мавлютиновичу Амербаеву. Это были нелёгкие годы перестройки, становления независимости Республики Казахстан и её науки.

Под руководством Вильжана Мавлютиновича была разработана концепция развития информатики в Казахстане, информатизации республики, в которой основной упор делался на увлечённость этим направлением молодых кадров.

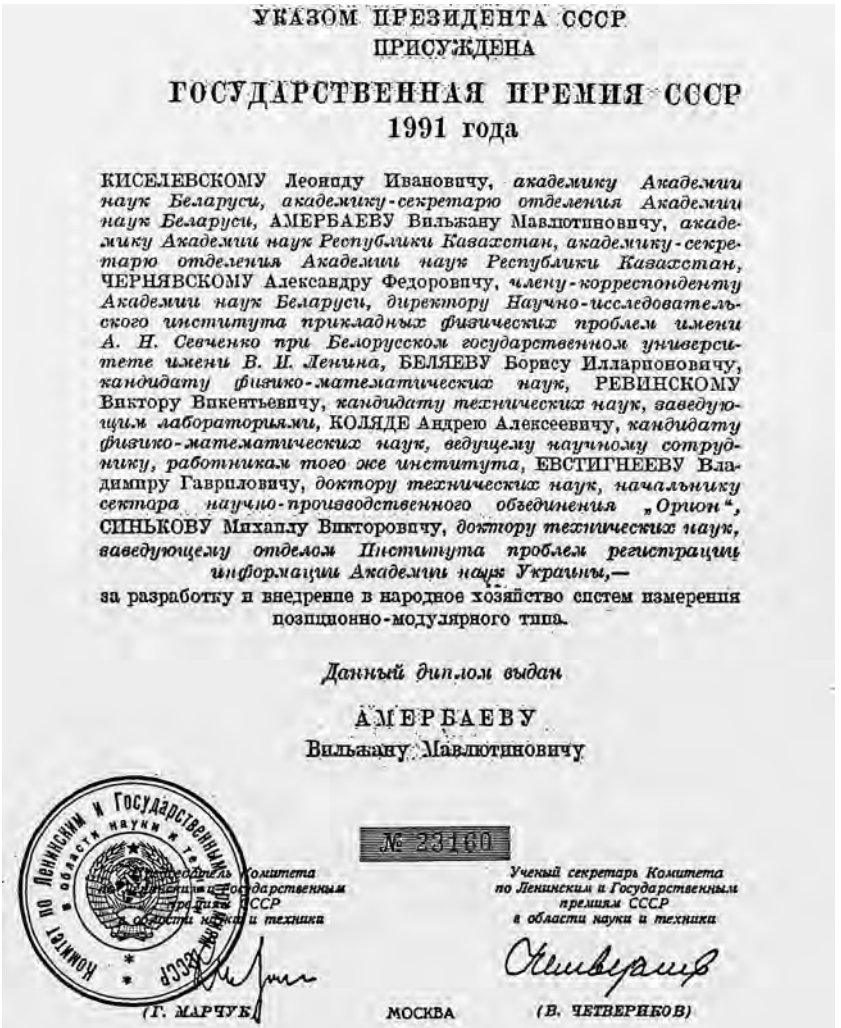
В 1991 году впервые в Казахстане усилиями Вильжана Мавлютиновича под его председательством создаётся специализированный диссертационный совет по защите докторов и кандидатов наук по двум специальностям: «вычислительные машины, системы и сети» и «алгебра и теория чисел».

Вильжан Мавлютинович подготовил для казахстанской науки около 30 кандидатов и докторов наук. В том что Институт математики при нём стал родоначальником пяти новых институтов, есть огромная заслуга В. М. Амербаева.

Вильжан Мавлютинович всегда находил время активно участвовать в пропаганде физико-математических знаний среди школьников и привлечении их через Малую академию наук (академия наук для школьников) к научным исследованиям через проведение различных научных конкурсов.

В 1991 г. Вильжан Мавлютинович был удостоен звания лауреата Государственной премии СССР по науке и технике «*за разработку и внедрение в народное хозяйство систем*

измерения позиционно-модулярного типа». Это была комплексная оценка вклада группы видных учёных России, Белоруссии, Украины и Казахстана, на основе совместных глубоких фундаментальных исследований в модулярной арифметике решивших важную для народного хозяйства проблему. И это было



УКАЗОМ ПРЕЗИДЕНТА СССР
ПРИСУЖДЕНА

ГОСУДАРСТВЕННАЯ ПРЕМИЯ СССР
1991 года

КИСЕЛЕВСКОМУ Леониду Ивановичу, *академику Академии наук Беларуси, академику-секретарю отделения Академии наук Беларуси*, АМЕРБАЕВУ Вильжану Мавлютиновичу, *академику Академии наук Республики Казахстан, академику-секретарю отделения Академии наук Республики Казахстан*, ЧЕРНЯВСКОМУ Александру Федоровичу, *члену-корреспонденту Академии наук Беларуси, директору Научно-исследовательского института прикладных физических проблем имени А. Н. Севченко при Белорусском государственном университете имени В. И. Ленина*, БЕЛЯЕВУ Борису Илларионовичу, *кандидату физико-математических наук*, РЕВИНСКОМУ Виктору Викентьевичу, *кандидату технических наук, заведующим лабораториями*, КОЛЯДЕ Андрею Алексеевичу, *кандидату физико-математических наук, ведущему научному сотруднику, работникам того же института*, ЕВСТИГНЕЕВУ Владимиру Гавриловичу, *доктору технических наук, начальнику сектора научно-производственного объединения „Орион“*, СИНЬКОВУ Михаилу Викторовичу, *доктору технических наук, заведующему отделом Института проблем регистрации информации Академии наук Украины,*—

за разработку и внедрение в народное хозяйство систем измерения позиционно-модулярного типа.

Данный диплом выдан

АМЕРБАЕВУ
Вильжану Мавлютиновичу

№ 23160

Председатель Комитета по Ленинским и Государственным премиям СССР в области науки и техники
(Г. МАРЧУК)

МОСКВА

Ученый секретарь Комитета по Ленинским и Государственным премиям СССР в области науки и техники
(В. ЧЕТВЕРИКОВ)

Из диплома о присуждении Государственной премии СССР

свидетельство высокой эффективности модулярной арифметики в определённом классе задач.

В 1994 году в Институте теоретической и прикладной математики (ИТПМ) начала работать междисциплинарная программа «Динамический хаос в распределённых системах». Инициатором и руководителем программы был Вильжан Мавлютинович.

В те же годы Вильжан Мавлютинович увлёкся «вечной» проблемой универсальности генетического кода и предложил модулярную арифметику в качестве эффективного инструмента его исследований.

Это примеры деятельности В. М. Амербаева только в качестве академика-секретаря и учёного в эти годы.

Но в 1992–1994 гг. в НАН РК в результате напряжённой внутренней борьбы произошла смена руководства. Вместо математика У. М. Султангазина был избран лидер конкурирующей «партии» экономист К. А. Сагадиев. Соответственно, в академии прошла волна смены многих руководителей.

Коснулась она и В. М. Амербаева, тесно сотрудничавшего со ставшим неугодным У. М. Султангазиным. Он был освобождён от должности академика-секретаря и члена президиума академии и переведён в институт теоретической и прикладной математики на должность заведующего лаборатории автоматизированных систем цифровых данных (ЛАСЦД).

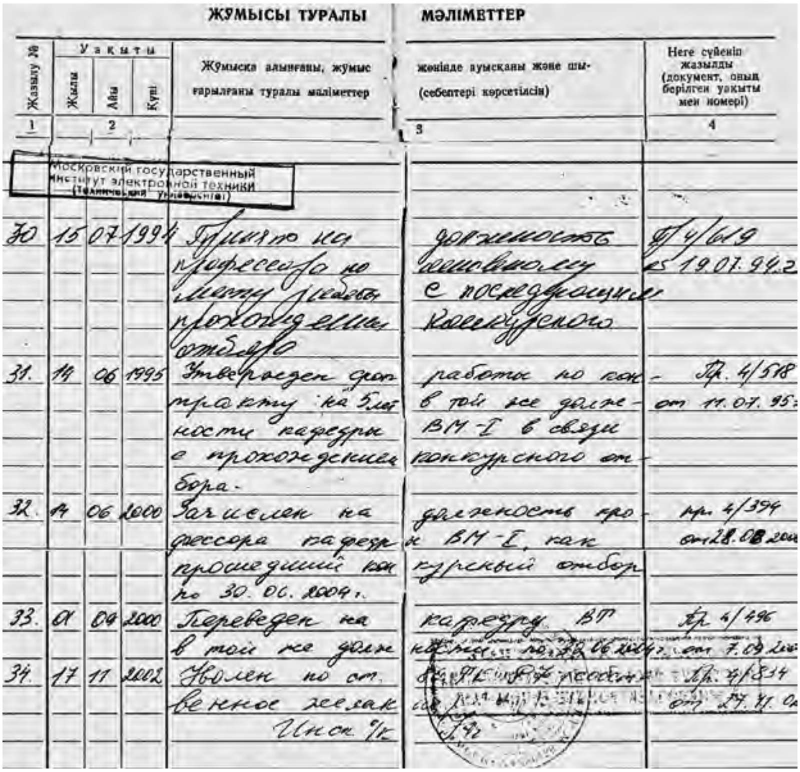
В этих условиях Вильжан Мавлютинович счёл невозможным для себя продолжение работы в структурах НАН РК и вернулся в Зеленоград. Окончательно. Но продолжал контакт со многими казахстанскими учёными — друзьями и уважаемыми им коллегами.

Зеленоград, МИЭТ, 1994–2002 гг.

15 июля 1994 г. В. М. Амербаев был принят в МИЭТ на должность профессора кафедры ВМ-1.

По результатам конкурса срок его полномочий до следующего конкурса был 30 июня 2004 г.

В течение 26 лет в два этапа Вильжан Мавлютинович преподавал студентам МИЭТа высшую математику, руководил аспирантами, проводил научные исследования и разработки.



ЖҰМЫСЫ ТУРАЛЫ МӘЛІМЕТТЕР

Жазылу №	Уақыты: Жылы	Айы	Күні	Жұмысқа алынғаны, жұмыс жөнінде ауысқаны және шығарылғаны туралы мәліметтер (себептері көрсетілсін)	Негіз сүйеніп жазылды (документ, оның берілген уақыты мен номері)
1	2			3	4
				Московский государственный институт электронной техники (Технический университет)	
30	15	07	1994	Принят на должность профессора по ... с последующим прохождением конкурсного отбора	Пр. 4/619 от 19.07.94 г.
31.	14	06	1995	Утвержден по контракту на 5 лет работы по контракту в той же должности кафедры ВМ-I в связи с прохождением конкурсного отбора.	Пр. 4/578 от 11.07.95 г.
32.	14	06	2000	Зачислен на должность профессора кафедры ВМ-I, как прошедший конкурсный отбор по 30.06.2004 г.	Пр. 4/394 от 28.08.2000
33.	01	09	2000	Переведен на кафедру ВТ в той же должности по 28.06.2004 г.	Пр. 4/496 от 7.09.2000
34.	17	11	2002	Уволен по собственному желанию ст. 80 ТК РФ. Инсп. ОК	Пр. 4/834 от 27.11.02

Из трудовой книжки: 1994–2002 гг. — МИЭТ ТУ

Многие из его учеников с благодарностью вспоминают (в т.ч. и в настоящем сборнике) своего уникального учителя и наставника, отмечая его высокую профессиональность и как математика, и как педагога. А также его высочайшие человеческие качества.

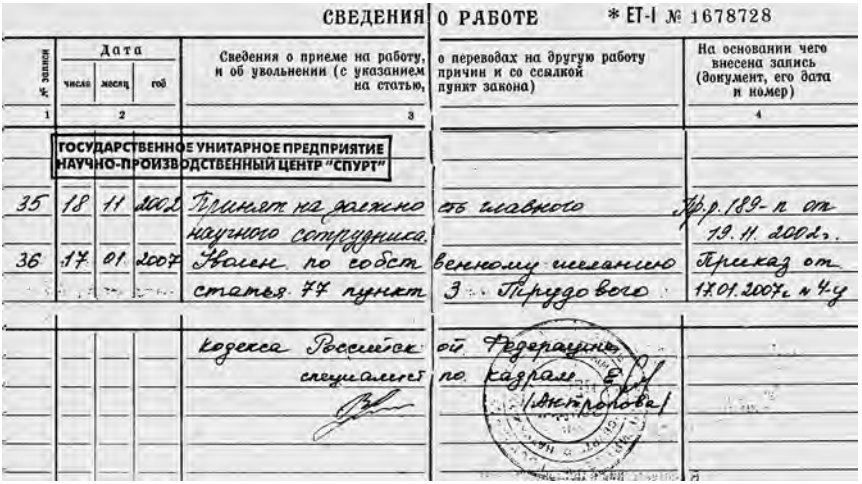
Представлен В.М. Амербаев и на доске почёта МИЭТа среди лауреатов Государственной премии.

Но в 2002 г. В.М. Амербаев встретился с коллегой-СВЦ-шником Е.М. Зверевым и узнал, что в Зеленограде есть интересная для него сложная математическая проблема. В результате он перешёл на работу в научно-производственный центр «СПУРТ», но до последнего своего дня продолжал преподавательскую работу в МИЭТе по совместительству.

Фрагмент доски почёта ТУ МИЭТ. Рядом с В. М. Амербаевым — нынешний (2019 г.) ректор МИЭТа В. А. Беспалов

Зеленоград, «СПУРТ», 2002–2007 гг.

18 декабря 2002 г. В. М. Амербаев был принят на должность главного научного сотрудника государственного унитарного предприятия НПЦ «СПУРТ».



СВЕДЕНИЯ О РАБОТЕ * ЕТ-I № 1678728

№ записи	Дата: число	Дата: месяц	Дата: год	Сведения о приеме на работу, и об увольнении (с указанием на статью,	о переводах на другую работу причин и со ссылкой пункт закона)	На основании чего внесена запись (документ, его дата и номер)
1	2			3		4
	ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР "СПУРТ"					
35	18	11	2002	Принят на должность научного сотрудника.	Из главного	Пр. р. 189-п от 19.11.2002 г.
36	17	01	2007	Уволен по собст. статья 77 пункт 3 Кодекса Российск. специалист	венному желанию Трудового	Приказ от 17.01.2007 г. № 4-у

Из трудовой книжки: 2002–2007 гг. — «СПУРТ»

В. М. Амербаев в группе ведущих разработчиков супер-ЭВМ 5Э53 в СВЦ в день 75-летия Д. И. Юдицкого, 22.09.2004 г. Слева направо: Хайков В. С., Рыков Л. Г., Корнев М. Д., Белова М. Н., Хорьков Р. В., Амербаев В. М.

Одной из задач НПЦ «СПУРТ» в то время было создание средств защиты компьютерной информации от несанкционированного доступа. Перед Вильжаном Мавлютиновичем была поставлена задача математической проработки способов улучшения характеристик (быстродействие, надёжность, защищённость и др.) этих средств.

В 2004 г. бывшие СВЦ-шники встретились в 75-ю годовщину Д. И. Юдицкого. В 2006 г. в «СПУРТ» было проведено уточнение тематики с соответствующей реорганизацией предприятия. В результате ряд ведущих специалистов в области защиты

информации, в т. ч. и В. М. Амербаев, сконцентрировались в зеленоградской фирме «АНКАД», основной тематикой которой была именно защита информации.

Зеленоград, фирма «АНКАД», 2007–2014 гг.

Сам Вильжан Мавлютинович в АНКАД устроился на работу «по совместительству», поскольку уже имел договорённость о поступлении на постоянную работу в ИППМ РАН. Поэтому в его трудовой книжке отражения работы в фирме «АНКАД» нет, а в качестве иллюстрации мы привели запись о приёме на работу из его личного дела. Но и этой работе, как и всему в его жизни, Вильжан Мавлютинович отдавался полностью и выполнял её до последнего дня.

III. ПРИЁМ НА РАБОТУ И ПЕРЕВОДЫ НА ДРУГУЮ РАБОТУ

Дата	Структурное подразделение	Профессия (должность), разряд, класс (категория) квалификации	Тарифная ставка (оклад), надбавка, руб.	Основание	Личная подпись владельца трудовой книжки
1	2	3	4	5	6
09.01.07		главный специалист		пр. №8 к от 09.01.07	

Из личного дела, «АНКАД»

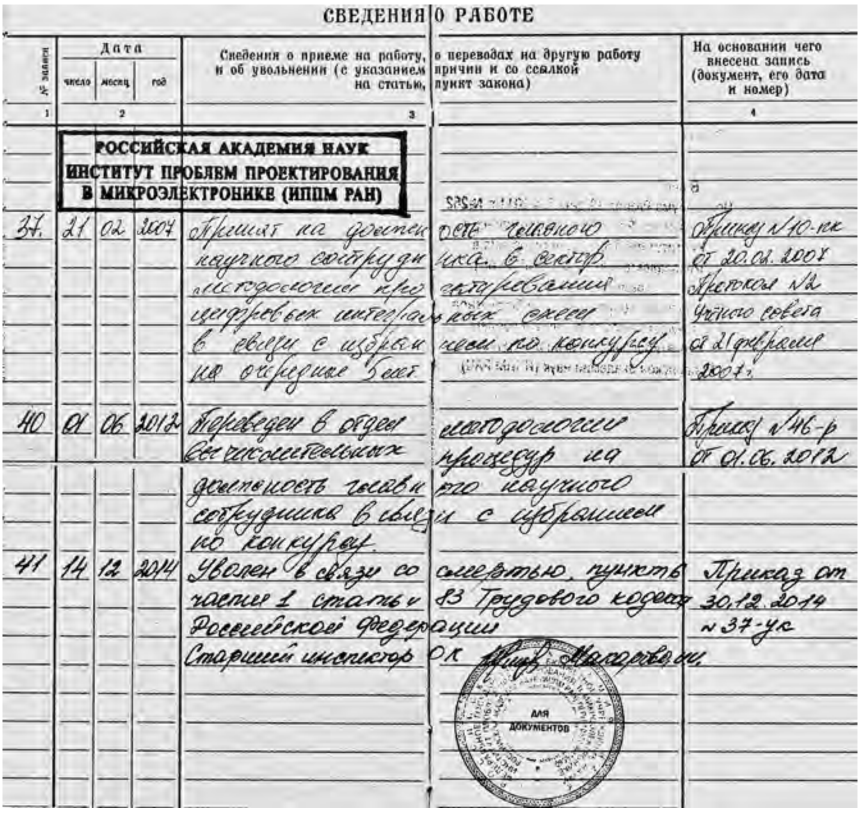
Зеленоград, ИППМ РАН, 2007–2014 гг.

ИППМ РАН, «АНКАД» и МИЭТ — последние места работы Вильжана Мавлютиновича.

При приёме на работу Вильжан Мавлютинович, как это было заведено ещё с советских времён, собственноручно заполнил личный листок по учёту кадров, приводим его 1-ю страницу.

В 2009 г. В. М. Амербаев, как всегда в таких случаях, вместе с коллегами из СВЦ отметил 80-летие Д. И. Юдицкого.

Как мы уже говорили, Вильжан Мавлютинович никогда не терял связей с алма-атинскими учёными. Проявляя глубокое к нему уважение, в 2005 г. они пригласили Вильжана Мавлютиновича на 40-летний юбилей Института математики и механики АН КазССР, в создании и развитии которого он принимал активнейшее участие.

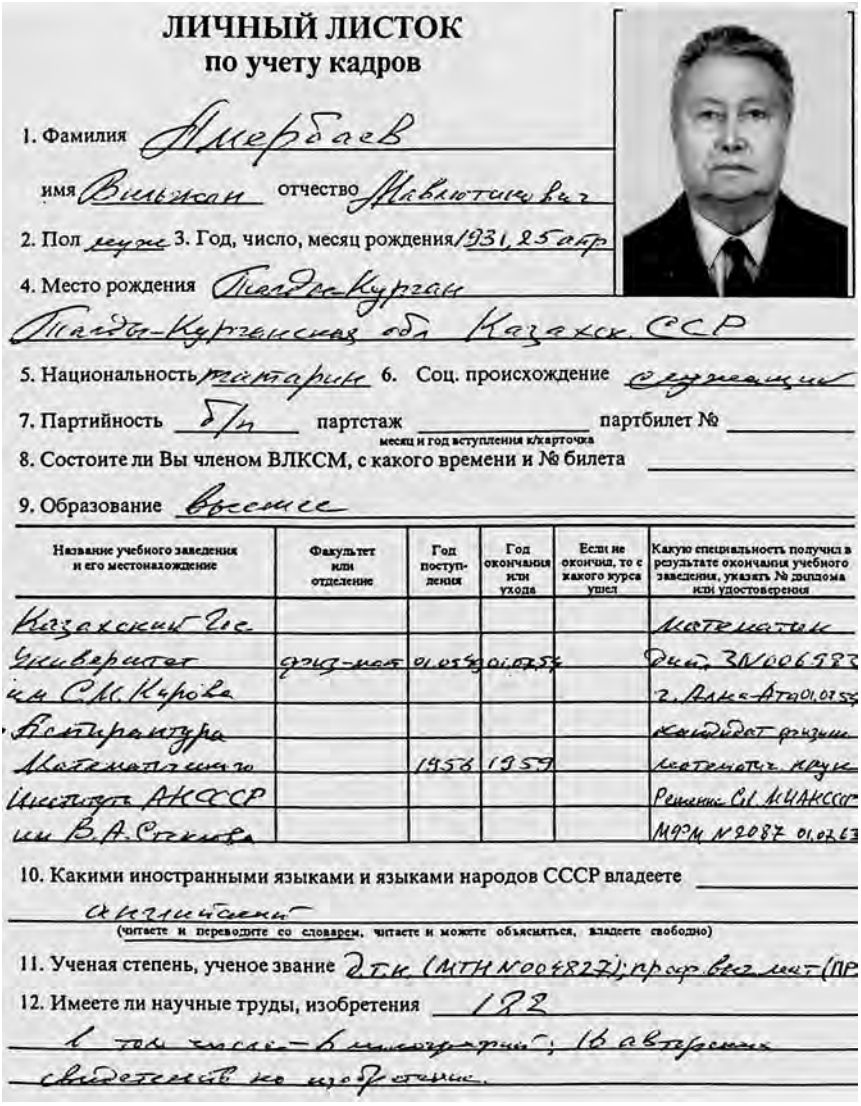


СВЕДЕНИЯ О РАБОТЕ

№ записи	Дата: число	месяц	год	Сведения о приеме на работу, о переводах на другую работу и об увольнении (с указанием причин и со ссылкой на статью, пункт закона)	На основании чего внесена запись (документ, его дата и номер)
1	2			3	4
				РОССИЙСКАЯ АКАДЕМИЯ НАУК ИНСТИТУТ ПРОБЛЕМ ПРОЕКТИРОВАНИЯ В МИКРОЭЛЕКТРОНИКЕ (ИППМ РАН)	
37.	21	02	2007	Принят на должность ведущего научного сотрудника в сектор методологии проектирования цифровых интегральных схем в связи с избранием по конкурсу на очередные 5 лет	Приказ № 10-лк от 20.02.2007 Протокол № 2 Ученого совета от 21 февраля 2007 г.
40	01	06	2012	Переведен в отдел вычислительных методологических процедур на должность главного научного сотрудника в связи с избранием по конкурсу	Приказ № 46-р от 01.06.2012
41	14	12	2014	Уволен в связи со смертью, пункт 6 части 1 статьи 83 Трудового кодекса Российской Федерации. Старший инспектор ОК [подпись] Макарова.	Приказ от 30.12.2014 № 37-ук

ДЛЯ ДОКУМЕНТОВ

Из трудовой книжки: 2007–2014 гг. — ИППМ РАН



ЛИЧНЫЙ ЛИСТОК
по учету кадров

1. Фамилия Амербаев
имя Вильжан отчество Павлютович
2. Пол муж. 3. Год, число, месяц рождения 1931, 25 апр
4. Место рождения Талды-Курган
Талды-Курганская обл Казахск. ССР
5. Национальность татарин 6. Соц. происхождение служащий
7. Партийность б/п партстаж _____ партбилет № _____
(месяц и год вступления к/карточка)
8. Состоите ли Вы членом ВЛКСМ, с какого времени и № билета _____
9. Образование высшее

Название учебного заведения и его местонахождение	Факультет или отделение	Год поступления	Год окончания или ухода	Если не окончил, то с какого курса ушел	Какую специальность получил в результате окончания учебного заведения, указать № диплома или удостоверения
Казахский Гос.					математик
Университет	физ-мат	01.09.50	01.07.54		Дип. ЗВ 006983
им С.М. Кирова					г. Алма-Ата 01.07.55
Аспирантура					кандидат физико-
Математического		1956	1959		математич. наук
Института АН СССР					Решение Сов. МИАН СССР
им В.А. Стеклова					МФМ № 2087 01.02.63

10. Какими иностранными языками и языками народов СССР владеете _____
английским
(читаете и переводите со словарем, читаете и можете объясняться, владеете свободно)
11. Ученая степень, ученое звание д.т.н. (МТН № 004827); проф. вед. мат. (ПР
12. Имеете ли научные труды, изобретения 122
1 под числом – 6 монографий; 16 авторских
свидетельств на изобретения.

Личный листок по учёту кадров в ИППМ

На 80-летии Д. И. Юдицкого, 23.09.2009.
В 1-м ряду: Отрохов Ю. Л., Дшхунян В. Л., Амербаев В. М.,
Коломыц В. Г.

На конференции, посвящённой 40-летию
Института математики и механики, Алма-Ата, 22.09.2005 г.
Второй справа — В. М. Амербаев, четвёртый — Р. Г. Бияшев

Вильжан, Олег (сын Наили), Лейла, Жан (сын Лейлы),
Алма-Ата, 2005 г.

Это был последний визит Вильжана Мавлютиновича в Алма-Ату, позволивший ему встретиться с многочисленными родственниками.

Но где бы Вильжан Мавлютинович ни работал, отвлечься от всех важных и необходимых производственных дел, полностью погрузиться в глубины любимой им математики он мог только дома, за своим рабочим столом, в окружении книг.

Главное рабочее место, дома

Семья

Ещё до поступления в университет Вильжан встретил Эмилию Петровскую и полюбил её раз и навсегда.

В 1952 г. они поженились.

Молодые Вильжан и Эмилия

Вильжан и Эмилия

С семьёй Вильжана мы уже познакомились, наступило время познакомиться с семьёй его верной спутницы жизни.

Семья Эмилии

Это была семья с очень интересной историей.

Бабушка Эмилии, Афанасьева Елена Евстафьевна 1885 г.р., с отличием закончила Херсонскую гимназию. У неё был молодой человек, и они собирались в дальнейшем обвенчаться. В это время в городе Херсоне активно работала подпольная группа, целью которой было свержение власти в городе. В состав группы входил дальний родственник Елены с той же фамилией Афанасьев. Группе удалось совершить покушение на главу города, но не удалось скрыться. И Фауст Кузьмич Афанасьев вместе с товарищами попал за решётку. По законам того времени их должны были повесить. Однако в законе был смягчающий пункт: если найдётся девица, которая согласится обвенчаться с преступником, то смертная казнь сменяется пожизненной каторгой.

Родственники Фауста в слезах умоляли Елену совершить акт милосердия и согласиться на брак с несчастным. Елена обвенчалась с ним и так спасла его от петли.

Сослали каторжников в Сибирь, в город Ачинск. В 1910 году в семье родился сын Виталий, а в 1912 — дочь Галина, будущая мать Эмилии.

После свержения самодержавия семья продолжала жить в Сибири, только перебрались в Томск. Фауст Кузьмич Афанасьев был очарован идеями всеобщего равенства и братства. В своих поступках он руководствовался ими. Так, однажды он вернулся домой в мороз без пальто, т. к. решил отдать его замерзающему человеку. Семья нуждалась в средствах, время было голодное, однако Фауст Кузьмич повесил на дереве объявление о бесплатном обучении детей. Елена была удивлена, когда к ней домой пришли бабы с ребятишками, желающими научиться грамоте. Она, конечно же, стала их учить бесплатно и, слава Богу, некоторые приносили в качестве оплаты продукты.

Елена со свёкром Кузьмой Афанасьевым — прадедом Эмилии

В 1919 году у Елены Евстафьевны родилась дочь Елена и тогда же скончался ее муж. Он работал в тифозном бараке, заразился и умер. Елена с детьми решила перебираться на юг. Сначала они переехали в Семипалатинск, а потом прибыли в Алма-Ату.

Афанасьева Елена Евстафьевна, бабушка Эмилии, около 1924 г., г. Семипалатинск

В Алма-Ате был острый дефицит кадров. Елена, с её блестящим образованием, стала работать в Центральном банке. Каждый день она надевала блузки разных оттенков: белую, розовую, голубую, салатовую, бежевую, кремовую, а костюм был единственный — из чёрного габардина. И все считали её богачкой, так хорошо она выглядела.

Дочь Галина вышла замуж за Петровского Нестора Михайловича.

Нестор родился в селе Еремеевка Полтавской губернии в 1900 году.

К моменту женитьбы на Галине Нестор был военным и служил музыкантом в НКВД. Отец и дед Петровские были золотых и серебряных дел мастерами. До и после революции семья жила достаточно зажиточно и дарила дорогие подарки своим родным. Во время Великой Отечественной войны Галина постепенно сдала все украшения в Торгсин (Всесоюзное объединение по торговле с иностранцами) — надо было кормить семью.

Нестор Михайлович и Галина Фаустовна, родители Эмилии

В 1930 году у них родилась дочь Эмилия. Но жизнь Галины с Нестором не сложилась, в 1933 г. они разошлись. Через несколько лет Галина вышла замуж за Грекова Ивана Александровича и у Эмилии родились ещё две сестры Наталья в 1936 г. и Людмила в 1938 г.

У Эмилии был характер лидера. Где бы она ни появлялась, всегда вокруг неё была весёлая компания парней и девушек. Эмилия мечтала стать учителем, но обстоятельства сложились так, что высшее образование она получила только будучи замужем. В 17 лет, после перенесённого тяжёлого заболевания, она сильно отстала по всем предметам. Постепенно она догнала сверстников, но математика никак ей не давалась. И тогда один

из её друзей сказал, что знает классного математика Вильжана. Они начали заниматься и влюбились друг в друга. Сначала, конечно, они дружили, а поженились только в 1952 году.

В 1960 г. Эмилия закончила заочное отделение Московского педагогического института им. В. И. Ленина по специальности «преподаватель географии».

В работе Вильжан был погружён в математику, и Эмилия занималась любимым делом — педагогикой. Она преподавала географию и была классным руководителем в алма-атинской школе № 25.

Три сестры: Эмилия, Людмила и Наталья

Однажды родители учеников сказали ей, что очень рады, что географию преподаёт учительница, которая так много сама путешествовала по всему миру. Эмилия Нестеровна очень удивилась и ответила, что никогда дальше Алма-Аты не уезжала. «*Откуда же Вы берете такую яркую информацию?*» — «*А я выписываю журнал «Вокруг Света»*. Эмилия могла своими рассказами

заинтересовать самых нерадивых учеников. Она организовала географический кружок, и там они составляли карту будущих путешествий. Все в классе любили географию.

Классный руководитель Эмилия Нестеровна
с учениками в Алма-Ате

С коллективом школы № 25 в Алма-Ате

В Зеленограде Эмилия Нестеровна работала в школе № 609 учителем географии и классным руководителем. Она так организовала работу в своём первом в этой школе 6 «Ж» классе, что по окончании учебного года он был признан лучшим в учёбе и общественной работе и награждён поездкой на теплоходе по каналу им. Москвы и по р. Оке в г. Горький (ныне Нижний Новгород). На этом корабле у всех учеников были свои функции, и к концу путешествия был готов судовой журнал с картами, фотографиями, рассказами и рисунками ребят. По приезде альбом, как отчёт по поездке, был вручён директору школы Борису Леонидовичу Яковлеву.

Семья Вильжана и Эмилии

У Вильжана и Эмилии родились две дочери: в 1953 г. Ирина и в 1963 г. Ольга.

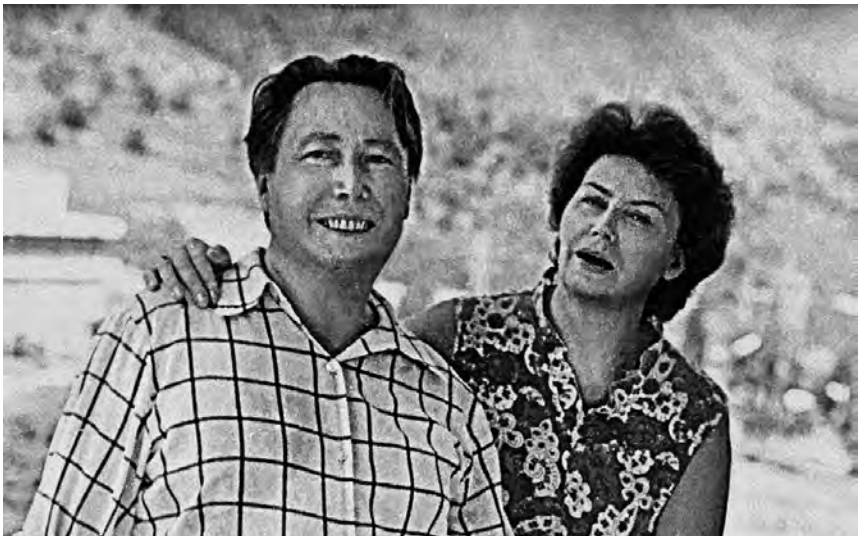
Эмилия Нестеровна с дочкой Ирой


Ира с мамой и Оля с папой


Вильжан и Ирина, Алма-Ата, 2005 г. Ольга, Зеленоград, 1985 г.

Дочки выросли, окончили вузы, Ирина — МИЭТ, Ольга — МГУ ВМК.

С семьёй в Кисловодске, 1976 г.



Вильжан и Эмилия, Алма-Ата, 1973 г.

Ирина Вильжановна

У Ирины родились дети — внуки Вильжана Мавлютиновича и Эмилии Нестеровны: Евгений и Майя.

Внуки тоже уже выросли, создали свои семьи и подарили бабушке и дедушке правнуков: Женя — Диму и Жанну, а Майя — Алису.

С внуком Женей, 1982 г., Женя в 2018 г.


С внучкой Майей, 1987 г., Майя, 2007 г.

Вся семья Вильжана Мавлютиновича и Эмилии Нестеровны живёт в Зеленограде.

Кстати, с Зеленоградом связала свою жизнь и троюродная сестра Вильжана — Наиля Расимовна Амирбаева 1949 года рождения. Она внучка брата Оспана — Омара. Окончив МИЭТ в первом выпуске, она всю жизнь проработала в Зеленограде.

Её дочь, Медведева Елена Викторовна, — талантливый врач-ветеринар. Она закончила Московскую государственную академию ветеринарной медицины и биотехнологии им. К. И. Скрябина и всю свою жизнь связала со спасением животных. Получив грант в 2001 г., Елена продолжила образование в Германии, в Университете Карлсруэ по специальности «экология и паразитология», для чего специально выучила немецкий язык.

Наиля Расимовна Амирбаева

Правнуки Дима (2006 г. р.) и Алиса (2010 г. р.) в 2018 г.

Ольга Вильжановна

У Ольги тоже родились дети — внуки Вильжана Мавлютиновича и Эмилии Нестеровны: Аня (1991 г.) и Лена (1998 г.).

С внучкой Аней, 1995 г., Аня, 2009 г.

С внуками Майей, Женей и Леной, 2002 г.

Внучка Лена со своей работой, 2017 г.

Все дети и внуки Вильжана Мавлютиновича и Эмилии Нестеровны получили высшее образование по выбранным ими

специальностям и успешны каждый в своём деле. Но интерес Вильжана Мавлютиновича унаследовала только дочь Ольга, выбравшая математику своей специальностью.

Друзья

У Вильжана и Эмилии было немало друзей и ещё больше приятелей.

Вернейшим и вечным другим Вильжана, а затем и Эмилии был Иван Тимофеевич Пак, с которым они познакомились на приёмных экзаменах в КазГУ в 1949 г.

С алма-атинскими гостями в зеленоградском лесопарке, 1967 г.
Стоят слева направо: Анвар Амирбаев — младший брат Вильжана;
Костя Кирпичников — двоюродный брат Эмилии;
Саша Калифатиди — сын Евгении Константиновны,
доброй подруги семьи Амербаевых. Сидят справа налево: Вильжан;
Евгения Константиновна Калифатиди; Эмилия с Олей;
Александра Федоровна Барвенко — завуч алма-атинской школы,
подруга Эмилии со своей дочкой Светой; Ира;
Валерий Александрович Огарков — муж Людмилы,
сестры Эмилии и перед ними Людмила Ивановна Огаркова

Где бы они ни жили, всегда к ним приходили гости, и они сами любили встречаться и путешествовать с друзьями.

Как-то летом к ним в Зеленоград приехали родные и друзья. В 3-комнатной квартире уместилось 12 человек!

В зеленоградской квартире у Амербаевых часто собирались гости. К ним приходили Панайоти Борис Николаевич с женой Гуровой Антониной Карповной, Ладыженские Даниил Бенционович и Валентина Дмитриевна. Частыми гостями были семья Сафоновых Антонины Георгиевны и Виктора Авраамовича, Пьянзина Людмила Яковлевна, Касимовы Юрий и Татьяна, Шершановские Ирина Алексеевна и Илья Михайлович. К ним часто приходили Юдицкий Давлет Исламович и Акушский Израиль Яковлевич. Гости очень любили манты, которые Эмилия Нестеровна мастерски готовила для гостей.

С Б. Н. Панайоти на демонстрации и Л. Я. Пьянзина

Отдых

В молодости Вильжан и Эмилия любили путешествовать. Однажды большой компанией на двух машинах они отправились путешествовать на озеро Боровое в Казахстане.

Не прекращал Вильжан Мавлютинович человеческих и научных связей с зеленоградцами, посещая СВЦ и принимая зеленоградцев.

На озере Боровое в Казахстане, 1975 г.

Регулярно ездили в горы Заилийского Алатау (Пёстрые горы), у подножия которых расположена Алма-Ата.

С Эмилией в Цхалтубо, 1958 г.

В горах под Алма-Атой — выездной семинар любителей СОК:
1 — Амербаев В. М., 2 — Юдицкий Д. И., 3 — Акушский И. Я.,
4 — Амербаева Э. Н.


Эмилия Нестеровна (Зеленоград, 2010 г.) и Вильжан Мавлютинович (Алма-Ата, 2005 г.)

Все свои годы Вильжан Мавлютинович напряжённо трудился на благо любимой математики, а через неё и своей страны, своей Родины. Скрупулёзно и непрерывно. Всегда к месту произнося слова «Родина», «страна», «Отчизна» без какого-либо пафоса, естественно.

Но всему когда-то приходит конец, «тянуть сразу три воза»[4] становилось не по силам.

---

[4] До последнего своего дня Вильжан Мавлютинович работал в трёх местах: в ИППМ РАН и (по совместительству) в фирме «АНКАД», а также преподавал в МИЭТе.

Эмилия Нестеровна и Вильжан Мавлютинович дома в Зеленограде, 1998 г.

К середине 2014 г. Вильжан Мавлютинович пришёл к выводу, что пора менять свою жизнь, пора переходить на домашний режим работы, по своей программе, не связанной с производственными планами предприятий. Он планировал упорядочить все свои наработки в математике, выстроить их в единую сбалансированную систему.

Но не успел. 14 декабря 2014 г. внезапно, «на ходу» он ушёл из жизни.

Зеленоград и зеленоградцы с горечью узнали о невосполнимой утрате. И сделали то последнее, что ещё могли для него сделать — Вильжан Мавлютинович упокоился на «нулевом» участке центрального зеленоградского кладбища недалеко от своего друга Д. И. Юдицкого, от коллеги Л. Н. Преснухина, среди выдающихся людей города.

Последнее пристанище на Земле

ISSN 2077-7353

Вестник

МОСКОВСКОЙ ГОСУДАРСТВЕННОЙ АКАДЕМИИ ДЕЛОВОГО АДМИНИСТРИРОВАНИЯ

МГАДА

«Информационные технологии в области делового администрирования нуждаются в защите от случайных воздействий и внешних посягательств, что обусловливает необходимость не только глубокого понимания будущими специалистами проблем информационной безопасности, но и знания методов и средств их решения».

В. М. Амербаев, доктор технических наук, профессор вычислительной математики, академик НАН РК, лауреат Государственной премии СССР по науке и технике

№ 1 (20) / 2013

Серия

«ЭКОНОМИКА»

ГЛАВА 3

НАУЧНОЕ НАСЛЕДИЕ В. М. АМЕРБАЕВА

Научное наследие В. М. Амербаева представлено в его учениках и научных трудах, большая часть которых опубликована в различных изданиях.

Под учениками понимаются аспиранты и докторанты, у которых Вильжан Мавлютинович был либо научным руководителем, либо научным консультантом, либо официальным оппонентом. К ученикам относятся также его младшие сотрудники при выполнении научно-исследовательских и опытно-конструкторских разработок на предприятиях.

Редакционной группе не удалось восстановить полный список и даже количество учеников В. М. Амербаева, защитивших под его руководством кандидатские и докторские диссертации. По свидетельству заместителя главного учёного секретаря президиума АН КазССР 1969–1994 гг. Н. В. Ниретиной (т. е. человека осведомлённого), «*Вильжан Мавлютинович подготовил для казахстанской науки около 30 кандидатов и докторов наук*». Нет оснований считать, что в Зеленограде их было меньше. Следовательно, общее число только защитивших диссертации учеников Вильжана Мавлютиновича можно оценить как более 60 человек. А общее количество учеников значительно больше.

Возникли проблемы и при восстановлении перечня научных трудов В. М. Амербаева. Но о них в разделе «Библиография В. М. Амербаева».

Библиография В. М. Амербаева

Малашевич Б. М.

Активная научная деятельность В. М. Амербаева нашла отражение в его научных трудах. Но строгого их учёта Вильжан Мавлютинович не вёл. В его официальном «*Списке научных трудов и изобретений*» в личном деле по последнему месту работы в ИППМ РАН числится 120 трудов, в т. ч. 6 монографий. Очевидно, что реально их было значительно больше.

При подготовке книги пришлось провести восстановление перечня научных трудов В. М. Амербаева. Но полностью этого сделать, по-видимому, не удалось, поскольку постоянно всплывали всё новые и новые работы, а время подготовки книги ограничено. Всего удалось восстановить 220 научных трудов, подготовленных Вильжаном Мавлютиновичем за 56 лет научной деятельности. Их распределение по годам и видам трудов приведено на гистограмме (рис. 1).

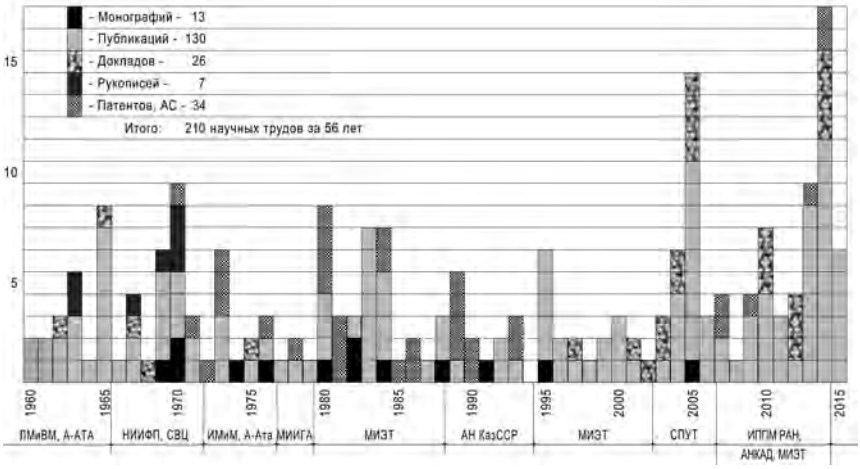


Рис. 1. Гистограмма распределения научных трудов В. М. Амербаева

Гистограмма показывает, что свои научные труды в виде отчётов по результатам выполнения многочисленных научно-исследовательских и опытно-конструкторских работ,

производственных докладов и т. п. он учитывал только в первые годы своей деятельности (до 1970 г., всего семь работ).

Похоже, он не очень ценил и выступления на конференциях, их указано всего 26, причём с большим временным разрывом — в период с 1976 по 1997 гг. (в течение 21 года) ни одной конференции, что практически невероятно. Возможно, не сохранилась информация.

34 авторских свидетельства на изобретения и патента, примерно равномерно распределённых в течение его научной деятельности, свидетельствуют о том, что его глубокие фундаментальные научные исследования регулярно приводили к новым техническим решениям, реализуемым в практическом приборостроении.

Гистограмма показывает резкий взлёт научной активности Вильжана Мавлютиновича в последние годы жизни. Он как будто спешил успеть сделать всё задуманное. Но не успел. Ряд публикаций вышли посмертно, в т. ч. в настоящем сборнике.

Далее рассмотрим полную, насколько её удалось восстановить, библиографию Вильжана Мавлютиновича. Его научные труды (выделены монографии) представлены в хронологическом порядке.

Перечень публикаций В. М. Амербаева

Монографии[1]

1. Амербаев В. М. и др. РТМ 410.012.003. Двухступенчатая непозиционная арифметика. — Москва, СВЦ, 1969.
2. Амербаев В. М. и др. РТМ У10.012.003 ред. 2–70. Машинные алгоритмы двухступенчатой непозиционной арифметики. — Москва, СВЦ, 1970.

---

[1] Монография — научное или научно-популярное издание, содержащее полное и всестороннее исследование одной проблемы или темы и принадлежащее одному или нескольким авторам.

Источник: словарь-справочник терминов нормативно-технической документации.

3. Акушский И. Я., Амербаев В. М., Пак И. Т. Основы машинной арифметики комплексных чисел. — Алма-Ата: Наука, 1970. — 248 с.
4. Амербаев В. М. Операционное исчисление и обобщённые ряды Лагерра. — Алма-Ата: Наука, 1974. — 181 с.
5. Амербаев В. М. Теоретические основы машинной арифметики. — Алма-Ата: Наука, 1976. — 323 с.
6. Амербаев В. М., Васильев В. И., Гуревич И. М., Пак И. Т. Распределение регулярных потоков сообщений в информационных системах. — Алма-Ата: Наука, 1980. — 143 с.
7. Амербаев В. М., Кальней А. Г., Клюшин А. В., Понайоти Б. Н., Ревякин А. М. Сборник задач по курсу «Алгоритмы и вычислительные методы: Учебное пособие. — М.: МИЭТ, 1982. — 118 с.
8. Амербаев В. М., Утембаев Н. А. Численный анализ лагерровского спектра. — Алма-Ата: Наука, 1982. — 186 с.
9. Амербаев В. М., Пак И. Т. Параллельные вычисления в комплексной плоскости. — Алма-Ата: Наука, 1984. — 182 с.
10. Амербаев В. М., Понайоти Б. Н. Неопределённый интеграл. Методические указания для самостоятельной работы по курсу «Основы математического анализа». — М.: МИЭТ, 1988. — 28 с.
11. Амербаев В. М., Ашимов А. А., Сарыабеков Ж. С. Информатизация республики: концепции и проблемы [Аналитический обзор]. — Алма-Ата: КазНИИНТИ, 1991. — 88 с.
12. Amerbaev Viljan, Kim Chil, Pack I. T. Theoretical Basises of Computer Arithmetic's. Seoul, Kwang Woon Universite, Korea, 1995, 220.
13. Амербаев В. М., Малашевич Б. М. (авторы-составители). Сб. трудов «50 лет модулярной арифметике. Юбилейная Международная научно-техническая конференция». — М.: МИЭТ, 2005. — 774 с.

Понятию «монография» соответствуют ещё шесть работ (поз. 39, 46, 51, 52, 53, 119 по библиографии) — это отчёты по НИР и ОКР, изданные в нескольких экземплярах и отнесённые к категории рукописей.

Научные публикации и изобретения

14. Амербаев В. М. Некоторые применения ортогональных многочленов к восстановлению функций, заданных изображением Лапласа. — Алма-Ата: Известия АН КазССР, сер. «Математика и механика», 1960. — Вып. 9.
15. Амербаев В. М. К вопросу о вычислении интерполяционного многочлена Чебышева // Вестник АН КазССР, 1960. — № 11. — 4 с.
16. Амербаев В. М. К вопросу о вычислении интерполяционного многочлена Чебышева // Инженерно-физический журнал, 1961. — Т. IV. — № 1.
17. Амербаев В. М. О конечном преобразовании Лапласа // Инженерно-физический журнал, 1961. — Т. IV. — № 1.
18. Амербаев В. М. Некоторые применения ортогональных многочленов к численному обращению интеграла Лапласа // Труды 2-й республиканской конференции по математике и механике. — Изд. АН КазССР, 1962.
19. Амербаев В. М. Об одном классе многочленов, ортогональных в комплексной области // Вестник АН КазССР, 1962. — № 5.
20. Амербаев В. М. Об одном модифицированном преобразовании Меллина // Вычислительная математика и математическая физика, 1962. — Т. II. — № 2. — С. 336–340.
21. Амербаев В. М. Некоторые численные методы обращения интегрального преобразования Лапласа, Алма-Ата, Рукопись диссертации. — Алма-Ата, 1963. — 200 с.
22. Амербаев В. М. Некоторые численные методы обращения интегрального преобразования Лапласа: Автореферат дисс. на соискание учен. степени кандидата физ.-мат. наук / Акад. наук СССР. Матем. ин-т им. В. А. Стеклова. — Москва [б. и.], 1963. — 16 с.
23. Амербаев В. М. О конечном преобразовании Лапласа. — Тепло и массоперенос, 1963. — Т. V. — Изд. АНБССР, 1963.
24. Амербаев В. М. Разложение функций оригиналов, заданных изображением Лапласа в ряды типа Неймана. — Труды сектора мат. и мех. АН КазССР, т. II «Вопросы диф. уравн. и мех. горных пород», 1963. — 20 с.

25. Амербаев В. М. Об одном модифицированном преобразовании Меллина // *U.S.S.R. Comput. Math. Math. Phys.*, **2**:2 (1963), 356–361. http://www.mathnet.ru/php/getFT.phtml?jrnid=zvmmf&paperid=7937&what=fullt&option_lang=rus.
26. Амербаев В. М. О движении за коммунистический труд в СО АН СССР // Вестник АН КазССР, 1964. — № 1. — 5 с.
27. Амербаев В. М. К теории операционного исчисления // Исследования по дифференциальным уравнениям и их применениям. — Алма-Ата: Наука, 1965.
28. Амербаев В. М. Об алгоритме восстановления функции-оригинала, когда изображение Лапласа является дробно-рациональной функцией с полюсами высокой кратности // Труды 1-й Казахстанской межвузовской конференции по математике и механике. — Наука, 1965.
29. Амербаев В. М. Н. Скобля. Таблицы для численного обращения преобразования Лапласа // *Ж. вычисл. матем. и матем. физ.*, 5:1 (1965), 166–167; *U.S.S.R. Comput. Math. Math. Phys.*, 5:1 (1965). — С. 244–245.
30. Амербаев В. М., Каипов Д. К. Резонансное рассеивание γ-квантов на ядрах // Журнал экспериментальной и теоретической физики, 1965. — Т. 48. — Вып. 5.
31. Амербаев В. М., Наурзбаев Ж. Н. О включении в пространство оригиналов функций с неинтегрируемой степенной особенностью // Исследования по дифференциальным уравнениям и их применениям. — Алма-Ата: Наука, 1965. — 10 с.
32. Амербаев В. М., Наурзбаев Ж. Н. О многочленах, ортогональных по свёртке // Известия АН КазССР, серия «Математика и механика», 1965. — № 3.
33. Амербаев В. М. Некоторые приёмы численного обращения преобразования Лапласа // Операционное исчисление. — М.: Наука, 1965.
34. Амербаев В. М. Рецензия на книгу Скобля «Таблицы узлов...» // Вычислительная математика и мат. физика, 1965. — № 1.

35. Амербаев В. М., Пак И. Т. Некоторые вопросы непозиционной системы счисления с комплексными основаниями // Известия АН КазССР, сер. физ-мат, 1965. — № 5. — 8 с.
36. Амербаев В. М., Наурзбаев Ж. Н. К вопросу об улучшения сходимости рядов Лагерра // Вестник АН КазССР, 1966. — № 12.
37. Амербаев В. М., Овчинников В. С. АС «Пороговое устройство», № 1205456 от 21.12.1967.
38. Амербаев В. М., Пак И. Т. О построении системы счисления остаточных классов в кольце главных идеалов // Труды министерства обороны, 1967. — № 75. — 18 с.
39. Амербаев В. М. Отчёт по теме «Алмаз». — Москва, НИИФП-СВЦ, 1967.
40. Амербаев В. М., Джаембаев Р. Т. Об одном классе функций типа спецфункций Ю. Н. Работнова // Вопросы механики горных пород. — Алма-Ата: Наука, 1967. — 15 с.
41. Амербаев В. М., Пак И. Т. Двоичная арифметика комплексных чисел // Материалы отчётно-научной конференции Института математики и механики АН КазССР. — Алма-Ата, 1968. — 7 с.
42. Амербаев В. М., Джаембаев Р. Т. Об одном представлении спецфункций Ю. Н. Работнова в замкнутой форме // Механические процессы в горном массиве. — Алма-Ата: Наука, 1969. — 10 с.
43. Амербаев В. М., Жаутыков О. А. Машинная арифметика в остаточных классах // Известия АН КазССР, серия физ-мат., 1969. — № 1. — 6 с.
44. Амербаев В. М., Пак И. Т. Двоичная система счисления с комплексными основаниями. — ВИНИТИ 1239-69, 1969.
45. Амербаев В. М., Пак И. Т. К вопросу о полных системах вычетов по комплексным модулям // Известия АН КазССР, серия физ-мат., 1969. — № 3. — 6 с.
46. Амербаев В. М. и др. Отчёт «Математическое обоснование машинных алгоритмов ЦВМ». — Москва, СВЦ. — 1969.

47. Амербаев В. М. и др. Пороговое логическое устройство. А. с. № 281900 от 3.07.1970.
48. Амербаев В. М., Джаембаев Р. Т. К теории многомерного дискретного преобразования Лапласа // Известия АН КазССР, серия физ-мат., 1970, 1. — 10 с.
49. Амербаев В. М., Наурзбаев Ж. Н. Разложение некоторых функций в ряды Лагерра // Известия АН КазССР, серия физ-мат., 1970, 3. — С. 56–63.
50. Амербаев В. М., Овчинников В. С. Определение позиционных характеристик чисел в системе счисления остаточных классов с помощью пороговой информационной системы // Кибернетика, 1970. — № 4. — 6 с.
51. Амербаев В. М. и др. Отчёт «Машинные алгоритмы». — Москва, СВЦ, 1970.
52. Амербаев В. М. и др. Отчёт «Моделирование машинных операций и алгоритмов». — Москва, СВЦ, 1970.
53. Амербаев В. М. и др. Отчёт по теме «Амур». — Москва, СВЦ, 1970.
54. Амербаев В. М. и др. Преобразователь кода из системы остаточных классов в полиадический код. А. с. № 328448 от 12.11.1971.
55. Амербаев В. М. Знак числа и немодульные операции в непозиционной системе счисления (СОК) // Электронная техника, сер. VI «Микроэлектроника», 1971. — Вып. 4 (30). — 12 с.
56. Амербаев В. М., Кокорин В. С. Распараллеливание операций округления в системе остаточных классов // Теория кодирования и информационного моделирования. — КазССР. — Алма-Ата: Наука, 1971 (73). — 6 с.
57. Амербаев В. М., Юдицкий Д. И., Акушский И. Я., Кокорин В. С., Седов В. С. Устройство для формирования позиционных признаков непозиционного кода. А. с. № № 365701 от 20.10.1972.
58. Амербаев В. М. и др. Устройство для округления чисел в системе остаточных классов. А. с. № 398949 от 21.06.1973.
59. Амербаев В. М., Кокорин В. С. и др. Устройство для формирования позиционных признаков непозиционного кода. А. с. 377766 от 22.01.1973.

60. Амербаев В. М., Акушский И. Я., Кокорин В. С., Захаров Ю. Л. Устройство для обнаружения и исправления ошибок в системе остаточных классов. А. с. № 398950 от 01.01.1973.
61. Амербаев В. М. Об одном способе обнаружения ошибок в системе остаточных классов // Теория кодирования и информационного моделирования. — КазССР. — Алма-Ата: Наука, 1973. — 9 с.
62. Амербаев В. М., Бияшев Р. Г. Интерполяция и коды, исправляющие ошибки // Теория кодирования и информационного моделирования. — КазССР. — Алма-Ата: Наука, 1973.
63. Амербаев В. М., Седов В. С. Оценка некоторых предельных соотношений для непозиционных кодов // Электронная техника, сер. VI «Микроэлектроника», 1973. — Вып. 4 (38). — 6 с.
64. Амербаев В. М., Баймульдина С. Б. Об одном полиноме, порождённом дробно-рациональной аппроксимацией функции e^{-s} // Известия АН КазССР, сер. физ-мат., 1975. — № 3 — 6 с.
65. Амербаев В. М., Черкасов Ю. Н., Бияшев Р. Г. Адаптивная система передачи данных по каналам космической связи // Сб. трудов III научн.-техн. конф. по космической радиосвязи, ИКИ АН СССР. — М., 1975.
66. Амербаев В. М., Бияшев Р. Г., Белова М. Н., Чепкасов Ю. Н., Альзамарова Э. И. Устройство для обнаружения и исправления ошибок арифметических преобразований полиномиальных кодов. А. с. № 542194 от 14.09.1976.
67. Амербаев В. М., Пак И. Т. Об одной концепции сжатия информации // Теория кодирования и оптимизация сложных систем. — Алма-Ата: Наука, 1976. — 6 с.
68. Амербаев В. М., Касимов Ю. Ф. О сравнении чисел в непозиционных системах счисления // Теория кодирования и оптимизации сложных систем. Алма-Ата: Наука, 1977. — С. 47–54.
69. Амербаев В. М. и др. Дешифратор кодов в системе остаточных классов. А. с. № 763889 от 18.02.1978 г.

70. Амербаев В. М., Касимов Ю. Ф. Формальная выразимость отношения порядка в алгебраических системах // Вестник АН КазССР, 1978. — № 11. — 5 с.
71. Амербаев В. М., Бияшев Р. Г., Белова М. Н. К вопросу об использовании кодов Лагранжа. Деп. ВИНИТИ. 19.01.79 № 258-79 // Автоматика и вычислительная техника, Рига: Зинатне, 1979. — № 4.
72. Амербаев В. М., Алексеенко А. Л. Об одном классе функциональных преобразований в модулярной арифметике // Теория кодирования и сложность вычислений. — Алма-Ата: Наука, 1980. — 5 с.
73. Амербаев В. М. и др. Преобразователь кода из системы остаточных классов в позиционный код. А. с. № 744549 от 30.06.1980.
74. Амербаев В. М., Евстигнеев В. Г. Дешифратор кодов в системе остаточных классов. А. с. № 763886 от 20.05.1980.
75. Амербаев В. М., Бияшев Р. Г., Карпухин А. И., Нугманов Р. Н. Устройство для исправления ошибок в корректирующих кодах. А. с. № 796848 от 15.09.1980 г.
76. Амербаев В. М., Бияшев Р. Г., Карпухин А. И., Нугманов Р. Н. Устройство декодирования с коррекцией ошибок. А. с. № 794728 от 08.09.1980 г.
77. Амербаев В. М. К вопросу об обобщении теоремы Котельникова — Шеннона // Методы цифровой обработки информации. — Москва: МИЭТ, 1980. — 8 с.
78. Амербаев В. М., Бияшев Р. Г., Евстигнеев В. Г., Черкасов Ю. Н. Устройство для обнаружения и исправления ошибок арифметических преобразований полиномиальных кодов. А. с. № 894711 от 01.09.1981 г.
79. Амербаев В. М., Бияшев Р. Г., Карпухин А. И., Нугманов Р. Н. Устройство для исправления ошибок в корректирующих кодах. А. с. № 903885 от 08.10.1981 г.
80. Амербаев В. М., Бородин В. Т. Устройство для формирования позиционных признаков модулярного кода. А. с. № 867178 от 21.05.1981 г.

81. Амербаев В. М. Анализ эквидистантных квадратур для интеграла Фурье // Методы цифровой обработки изображений. — М.: МИЭТ, 1982.
82. Амербаев В. М. Арифметические свойства кодов Рида — Соломона над кольцом вычетов по составному модулю. — Алма-Ата: Вестник АН КазССР, 1983. — № 7. — 8 с.
83. Амербаев В. М., Касимов Ю. Ф. Вычисления в алгебраических структурах // Численные методы решения задач математической физики и оптимизации. — Алма-Ата: Наука, 1983. — 16 с.
84. Амербаев В. М., Пак И. Т. Арифметические принципы кодирования комплексных чисел // ВИНИТИ, № 36-23-83 1983. — 9 с.
85. Амербаев В. М., Пак И. Т. Дискретные модели комплексных чисел // ВИНИТИ, № 37-22-83 1983. — 10 с.
86. Амербаев В. М., Пак И. Т. Модулярный БПФ-процессор. — Алма-Ата: Известия АН КазССР, физико-математическая серия, 1983. — 5 с.
87. Амербаев В. М., Пак И. Т. Параллельные вычисления значений аналитических функций. — Алма-Ата: Известия АН КазССР, физико-математическая серия, 1983. — 5 с.
88. Амербаев В. М., Пак И. Т. Структура Гауссова процессора // ВИНИТИ, № 45-52-83 1983. — 10 с.
89. Амербаев В. М. и др. Преобразователь непозиционного кода в позиционный код. А. с. № 1179546 от 6.04.1984.
90. Амербаев В. М., Пак И. Т. Параллельные вычисления линейной алгебры над комплексными числами // Вестник АН КазССР, 1984. — № 3. — 12 с.
91. Амербаев В. М., Пак И. Т. Принцип модулярности — основа распараллеливания ЦОС. — Алма-Ата: Известия АН КазССР, физико-математическая серия, 1984. — 7 с.
92. Амербаев В. М., Пак И. Т. Фильтры с конечной импульсной характеристикой в модулярной арифметике. — Алма-Ата: Известия АН КазССР, физико-математическая серия, 1984. — 10 с.

93. Амербаев В. М. Теорема Эфроса — Данилевского для Z-преобразований над кольцом // Микроэлектронные устройства и методы цифровой обработки информации. — М.: МИЭТ, 1984. — 10 с.
94. Амербаев В. М. и др. Арифметическое устройство в системе остаточных классов. А. с. № 1176326 от 27.03.1984.
95. Амербаев В. М. и др. Устройство для вычисления квадратного корня числа в модулярной системе счисления. А. с. № 1317434 от 25.11.1985.
96. Амербаев В. М. и др. Устройство для умножения чисел в модулярной системе счисления. А. с. № 1366878 от 02.07.1986.
97. Амербаев В. М., Коляда А. А. Устройство для умножения чисел в модулярной системе счисления. А. с. № 1368878 от 02.07.1986.
98. Амербаев В. М., Черных И. Н. Конструктивный метод повышения устойчивости к шумам алгоритма восстановления сигнала // Межвузовский сборник научных трудов. — М.: МИЭТ, 1987. — 6 с.
99. Амербаев В. М. Параллельные вычисления в кольце вычетов // Кибернетика и вычислительная техника. — Москва: Наука, 1988. — Вып. 4. — С. 170–177.
100. Амербаев В. М., Понайоти Б. Н. Неопределённый интеграл. Методические указания для самостоятельной работы по курсу «Основы математического анализа. — М.: МИЭТ, 1988. — 28 с.
101. Амербаев В. М. и др. Устройство для контроля информации в параллельном коде. А. с. № 1495800 от 23.07.1989.
102. Амербаев В. М., Бондаренко А. В. Особенности использования нетрадиционных машинных арифметик в бортовых системах обработки информации // Сб. Вычислительная техника в бортовых системах управления и обработки информации / Под ред. академика Федосова Е. А. — Москва, 1989. — 26 с.
103. Амербаев В. М., Пак И. Т. Устройство для формирования позиционного признака в модулярной арифметике. А. с. № 1532924 от 30.12.1989.

104. Амербаев В. М. Устройство для масштабирования чисел в модулярной арифметике. А. с. № 1541665 от 08.10.1989.
105. Амербаев В. М., Хлевной С. Н. Устройство для контроля информации в параллельном коде. А. с. № 1495-800 от 22.03.1989.
106. Амербаев В. М. и др. Устройство для масштабирования чисел в модулярной арифметике. А. с. № 1541605 от 7.02.1990.
107. Амербаев В. М., Пак И. Т. Преобразователь модулярного кода в позиционный. А. с. № 1587639 от 22.04.1990.
108. Амербаев В. М. Метод моментов для деконволюции // Вестник АН РК. — Алматы, 1992. — № 1. — 6 с.
109. Амербаев В. М. О сингулярных интегралах, фильтрующих отрезок ряда Тейлора // Доклады АН РК. — Алматы, 1992. — № 1. — 6 с.
110. Амербаев В. М., Пак И. Т. Позиционное кодирование комплексных чисел // ВИНИТИ, № 36-26-83, 1993. — 9 с.
111. Амербаев В. М., Пак И. Т., Бондаренко А. В. и др. Устройство для обнаружения и исправления ошибок. Патент СССР № 1827293, 30.08.1993. http://patents.su/patents/amerbaev.
112. Амербаев В. М., Пак И. Т. и др. Устройство для обнаружения и исправления ошибок. А. с. № 1837293 от 30.08.1993.
113. Amerbaev Viljan, Kim Chil. Analyses of Generalized Convolution by Method Z-Transformation over Ring // Reports National Academy of Sciences Republic of Kazakhstan, № 3, 1995.
114. Amerbaev Viljan. Arithmetization of Ride-Solomon's Codes // Reports National Academy of Sciences Republic of Kazakhstan, 1995. — № 3.
115. Амербаев В. М., Kim Chil. Z-преобразования над кольцом // Наука и техника, «Сотрудничество». — М., 1995. – № 2. — (на корейском языке).
116. Амербаев В. М., Pack I. T. Арифметизация... // Наука и техника, «Сотрудничество». — М., 1995. – № 2. — (на корейском языке).

117. Амербаев В. М., Макаренко Н. Г. Динамический хаос в распределённых системах // Сборник института теоретический и прикладной математики МН-АН РК. — Алматы, 1996. — 16 с.
118. Амербаев В. М. О математической спецификации универсального генетического кода // ДАН РК. — Алматы, 1996. — № 5. — 8 с.
119. Амербаев В. М., Кальней С. Г., Рычагов М. Н., Фролова Г. В. Исследование проблемы реставрации ультразвуковых медицинских изображений методами гомографной обработки цифровой аподизации / Отчёт по НИР. — М.: МИЭТ, 1997, РФФИ: 97-01-00686-а.
120. Амербаев В. М., Каримова Л. М. Методы детерминированного хаоса и криптостойкость алгоритмов шифрации // ИТПМ МК-АН РК «Динамический хаос». — Алматы, 1997 — Вып. 2. — 6 с.
121. Амербаев В. М., Пак И. Т. Позиционное кодирование комплексных чисел // ВИНИТИ, 1998. — № 36-26-83. — 9 с.
122. Амербаев В. М., Бархоткин В. А. О возможности определения скорости «бега местности» с помощью бортовой ПЗС-линейки сопровождения // Научные труды. — М.: МИЭТ, 1999. — 6 с.
123. Амербаев В. М., Бархоткин В. А. О повышении чувствительности прибора методом компенсации траекторных искажений // Научные труды. — М.: МИЭТ, 1999. — 6 с.
124. Амербаев В. М., Бархоткин В. А. К проблеме деконволюции в классе $W(N+1)$ // Информационные технологии и системы управления. — М.: МИЭТ, 2000. — С. 152–158.
125. Амербаев В. М., Матиец С. М. БПФ и шифросистема Хилла // Материалы международной научно-технической конференции «Электроника и информатика XXI века». — М.: МИЭТ, 2000. — 1 с.
126. Амербаев В. М., Бархоткин В. А. Курс криптологии на кафедре вычислительной техники МИЭТ // Известия вузов. Электроника. — М.: МИЭТ, 2000. — № 4–5. — С. 198–199.

127. Амербаев В. М., Кожухова Ю. И. Китайская теорема об остатках в кольце главных идеалов и ранцевая система шифрования // Материалы VII Международного семинара / Под ред. Лупанова Б. М. — Москва: Изд. ЦПИ, 2001. — 5 с.
128. Амербаев В. М., Матиец С. М. Кодовая защита от НСД матричных преобразований над конечным полем // Микроэлектроника и информатика. — М.: МИЭТ, 2001. — 6 с.
129. Амербаев В. М., Пак И. Т. Об одном варианте ускорения операции умножения кватернионов // Труды 9-х математических чтений МГСУ, секция «Математические методы и приложения». — Москва: МГСУ, 2002. — 3 с.
130. Амербаев В. М., Бияшев Р. Г. Модулярная криптосистема рюкзачного типа, V Международная конференция «Рус-Крипто 2003» по современной криптографии и системам защиты информации. — Москва, 2003. — 10 с.
131. Амербаев В. М., Грехнева И. Е. Об одном методе обеспечения конфиденциальности идентификаторов абонентов системы связи // VI Международная конференция «Рус-Крипто-2004» по современной криптографии и системам защиты информации. — Москва, 2004. — 25 с.
132. Амербаев В. М. Модулярная арифметика по бесконечной системе попарно взаимно-простых оснований // Приближение функций. Теоретические и прикладные аспекты. — М.: МИЭТ, 2003. — С. 51–57.
133. Амербаев В. М., Шарамок А. В. Метод построения программно-физического датчика случайный чисел // V Международная конференция «Рус-Крипто-2003» по современной криптографии и системам защиты информации. —Москва, 2003. — 10 с.
134. Amerbaev V. M., Kal'nej S.G., Rychagov M. N., Frolova G. V. Recovery of medical ultrasound images based on an effective deconvolution of scanning data // Медицинская техника, 2004. — № 3. — С. 9–12.
135. Restoration of medical ultrasonic images on the basis of effective deconvolution of scanning data / Amerbaev V. M., Kalnei S. G., Rychagov M. N., Frolova G. V. Biomedical Engineering, 2004. Т. 38. № 3. P. 116–119.

136. Амербаев В. М. и др. Реставрация медицинских ультразвуковых изображений на основе эффективной деконволюции данных сканирования // Медицинская техника, 2004. — № 3. — С. 9–12.
137. Амербаев В. М., Соловьев Р. А., Тельпухов Д. В., Балака Е. С. Построение обратных преобразователей модулярной арифметики с коррекцией ошибок на базе полиадического кода // Нейрокомпьютеры: разработка, применение, 2004. — № 9. — С. 30–35.
138. Амербаев В. М., Стемпковский А. Л., Широ Г. Э. Быстродействующий согласованный фильтр, построенный по модулярному принципу // Информационные технологии, 2004. — № 9. — С. 5.
139. Амербаев В. М., Бияшев Р. Г., Зверев Е. М. Модулярная модификация криптоалгоритма Хэллмана и её криптоанализ // Матер. VI Междунар. конф. «Рускрипто-2004». — М., 2004.
140. Амербаев В. М., Бияшев Р. Г. Алгоритмы Гаусса в задачах управления рандомизированной ключевой матрицей шифрсистемы Хилла // Доклады НАН РК, 2005. — № 1. — 4 с.
141. Амербаев В. М., Бияшев Р. Г., Нысанбаева С. Е. Применение непозиционных систем счисления при криптографической защите информации // Известия Национальной академии наук Республики Казахстан. Серия физико-математическая, 2005. — № 3. — С. 84.
142. Амербаев В. М., Горковенко Р. Г. Использование модулярной арифметики при формировании электронной подписи с заданными характеристиками // Доклады НАН РК, 2005. — № 4. — 8 с.
143. Амербаев В. М., Грехнева И. Е. Кластерная модель подсистемы защиты информации цифровых систем связи // 7-я Международная научно-практическая конференция «Информационная безопасность». — Таганрог, 2005. — С. 215–217.
144. Амербаев В. М., Бияшев Р. Г., Зверев Е. М., Щербаков А. Ю. Многопараметрическая модификация криптоалгоритма типа «ранец» // Вестник НАН РК. — Алматы, 2005. — № 1.

145. Амербаев В. М., Грехнева И. Е. Методы защиты от прослушивания 2-го рода в цифровых системах связи // 7-я Международная научно-практическая конференция «Информационная безопасность». — Таганрог, 2005. — С. 96–99.
146. Амербаев В. М., Грехнева И. Е. Система радиоуправления и радиомониторинга в подсистеме защиты глобальной системы спутниковой связи // Межотраслевой научно-технический журнал «Оборонный комплекс — научно-техническому прогрессу России». — Москва: ФГУПВИМИ, 2005. — № 2. — С. 77–80.
147. Амербаев В. М., Грехнева И. Е., Шарамок А. В. Кластерная модель подсистемы защиты информации цифровых систем связи // Информационное противодействие угрозам терроризма, 2005. — № 4. — С. 215–218.
148. Амербаев В. М., Грехнева И. Е., Шарамок А. В. Методы защиты от прослушивания второго рода в цифровых системах связи // Информационное противодействие угрозам терроризма, 2005. — № 5. — С. 96–101.
149. Амербаев В. М., Грехнева И. Е., Шарамок А. В. Система радиоуправления радиомониторинга в подсистеме защиты информации глобальной системы спутниковой связи // Оборонный комплекс — научно-техническому прогрессу России, 2005. — № 2. — С. 77–80.
150. Амербаев В. М., Дьячков В. Н. Модулярная арифметика как криптографический примитив: Сборник Научных трудов юбилейной международной научно-технической конференции. — Москва, 2005. — 9 с.
151. Амербаев В. М., Пак И. Т. Модулярной арифметике — 50 лет // Труды юбилейной Международной научно-конференции «50 лет модулярной арифметике». — Россия, Москва, Зеленоград, 23–25 ноября 2005. — М.: МИЭТ. — С. 5–22.
152. Амербаев В. М., Стемпковский А. Л., Широ Г. Э. Модулярный быстродействующий согласованный фильтр // Труды юбилейной Международной научно-конференции «50 лет модулярной арифметике». — Россия, Москва, Зеленоград, 23–25 ноября 2005. — М.: МИЭТ. — С. 250–267.

153. Амербаев В. М., Комиссаров А. В. SP-сети Фейстеля с управляемой структурой алгоритма // Методы проектирования и защиты мобильных систем связи. — М.: МИЭТ, 2006. — С. 91–99.
154. Амербаев В. М., Комиссаров А. В. Финитарный аналог стандартного отображения КАМ-теории в роли однораундовой схемы Фейстеля // Методы проектирования и защиты мобильных систем связи. — М.: МИЭТ, 2006. — С. 83–90.
155. Амербаев В. М., Шарамок А. В. Обеспечение имитозащищенности и конфиденциальности в системах радиосвязи // Методы проектирования и защиты мобильных систем связи. — М.: МИЭТ, 2006. — С. 70–76.
156. Амербаев В. М. Бияшев Р. Г., Зверев Е. М., Щербаков А. Ю. Модулярный ассиметричный криптографический алгоритм // Криптографические методы защиты информации / Под ред. Е. М. Сухарева // Научная серия «Защита информации». Кн. 4. — Москва: Радиотехника, 2007. Гл. 11. — С. 161–167.
157. Амербаев В. М., Зверев Е. М., Романец Ю. В., Шарамок А. В. Способ преобразования случайных чисел с произвольным законом распределения в случайные числа с равномерным законом распределения. Патент РФ № 2343628, приоритет от 11.01.2007. — 13 с.
158. Амербаев В. М., Романец Ю. В., Шарамок А. В. Способ криптографического преобразования блоков цифровых данных. Патент РФ № 2359415 С2, действует с 26.06.2007.
159. Амербаев В. М., Романец Ю. В., Тельпухов Д. В., Шарамок А. В. Способ суммирования маскированного числа со скрытым снятием маски в процессе суммирования. Патент на изобретение RUS 2372643 05.12.2007.
160. Амербаев В. М., Константинов А. В., Тельпухов Д. В. Бивалентный дефект модулярных кодов и выбор технологичных модулей, понижающий бивалентный дефект // III Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем — 2008». — Москва: ИППМ РАН, Сб. трудов, 2008 г. № 1. — С. 462–465.

161. Амербаев В. М., Малашевич Д. Б. Анализ эффективности реализации модульных операций индексной модулярной арифметики // Известия вузов. Электроника, № 6 (80), 2009. — С. 54–57.
162. Амербаев В. М., Романец Ю. В., Тельпухов Д. В., Шарамок А. В. Способ суммирования маскированного числа со скрытым снятием маски в процессе суммированияю Патент РФ № 2372643 (заявка от 05.12.2007, опубликовано 10.11.2009).
163. Амербаев В. М., Тельпухов Д. В., Шарамок А. В. Способ скрытого сложения и особенности его реализации // Известия вузов. Электроника, 2009. — № 3. — С. 26–32.
164. Амербаев В. М., Шарамок А. В. Синтез нелинейных отображений методом Гаусса // Известия вузов. Электроника, № 2 (76). — Москва, 2009. — С. 51–55.
165. Амербаев В. М., Балака Е. С. Анализ и синтез алгоритмов вычисления гауссовых логарифмов большого числа слагаемых над полем Галуа GF(p) // Изв. вузов. Электроника, 2010. — № 4. — С. 64–69.
166. Амербаев В. М., Балака Е. С. Методы вычисления гауссовых логарифмов N переменных над полем Галуа GF(p) // Известия вузов. Электроника, 2010. — № 4 (84). — С. 64–69.
167. Амербаев В. М., Балака Е. С., Константинов А. В., Тельпухов Д. В. Методы ускорения вычислений скалярных произведений векторов в базисе модулярной логарифметики // IV Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем — 2010». Сборник научных трудов под общ. ред. А. Л. Стемпковского. — Москва: ИППМ РАН, 2010. — № 1. — С. 378–381.
168. Амербаев В. М., Балака Е. С., Константинов А. В., Тельпухов Д. В. Методы построения прямых преобразователей модулярной логарифметики, ориентированной на ЦОС // IV Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем — 2010» // Сборник научных трудов под общ. ред. А. Л. Стемпковского. — Москва: ИППМ РАН, 2010. — С. 374–377.

169. Амербаев В. М., Корнилов А. И., Стемпковский А. Л. Модулярная логарифметика — новые возможности для проектирования модулярных вычислителей и преобразователей // IV Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем — 2010» // Сборник научных трудов под общ. ред. А. Л. Стемпковского. — Москва: ИППМ РАН, 2010. — С. 368–373.
170. Амербаев В. М., Максименко А. В. Модулярные рюкзачные преобразования в информационных технологиях // Информационные технологии, 2010. — № 5. — С. 30–33.
171. Амербаев В. М., Шарамок А. В. Криптографическое преобразование с двумерной сетевой структурой // Вопросы защиты информации, 2010. — № 3. — С. 12–16.
172. Amerbaev V. On Decomposition Theorem in Numerical Inversion Problem of Laplace Integral Transform // The 8th Congress of the ISAAK-2011, 2011. P. 196–209.
173. Amerbaev V., Balaka E. Modular Computations in the Algebra of Quadratic Matrixes of Order N. // The 8th Congress of the ISAAK-2011, 2011. P. 167–174.
174. Амербаев В. М., Кожухов И. Б., Ревякин А. М. Метод последовательного исключения переменных Гаусса в криптологии // Вестник Московской государственной академии делового администрирования. Серия «Философские, социальные и естественные науки», 2011. — № 5. — С. 137–142.
175. Амербаев В. М., Балака Е. С., Константинов А. В., Тельпухов Д. В. Реализация обратного преобразователя модулярной арифметики, совмещенного с операцией округления для задач ЦОС // V Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем — 2012» // Сборник научных трудов под общ. ред. А. Л. Стемпковского. — Москва: ИППМ РАН, 2012. — № 1. — С. 535–538.
176. Амербаев В. М., Балака Е. С., Константинов А. В., Тельпухов Д. В. Применение аппарата модулярной логарифметики для решения специальных задач матричной алгебры // V Всероссийская научно-техническая конференция

«Проблемы разработки перспективных микро- и наноэлектронных систем — 2012» // Сборник научных трудов под общ. ред. А. Л. Стемпковского. — Москва: ИППМ РАН, 2012. — № 1. — С. 539–542.

177. Амербаев В. М., Кожухов И. Б., Ревякин А. М. Представления бинарных отношений в теории измерений и полезности для оценки социального капитала // Вестник Московской государственной академии делового администрирования. Серия «Экономика», 2012. — № 4 (16). — С. 66–71.
178. Амербаев В. М., Стемпковский А. Л., Соловьев Р. А. Параллельные вычисления в кольце гауссовых чисел над полем Галуа GF(p) // V Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем — 2012» // Сборник научных трудов под общ. ред. А. Л. Стемпковского. — Москва: ИППМ РАН, 2012. — № 1. — С. 517–520.
179. Амербаев В. М. Модулярная арифметика сегодня // Малашевича Б. М. 50 лет отечественной микроэлектронике. Краткие основы и история развития. — М.: Техносфера, 2013. — С. 441–448.
180. Амербаев В. М. Тюфякин Д. Н., Шарамок А. В. Симметричное шифрование в режиме порундового сцепления. Статистический анализ стойкости // Вестник МГАДА. Серия «Экономика», 2013. — № 1 (20). — С. 21–28.
181. Амербаев В. М., Балака Е. С. Арифметическое устройство бимодульной арифметики конечного поля Галуа GF(p) // Research Journal of International Studies XX, 2013. — Ч. 2. — № 10 (17). — С. 5–9.
182. Амербаев В. М., Балака Е. С. Бимодульные вычисления над полем Галуа GF(p) // Вестник МГАДА. Серия «Экономика», 2013. — № 1 (20). — С. 36–42.
183. Амербаев В. М., Ревякин А. М. О некоторых аспектах теории и практики информационной безопасности в области делового администрирования // Вестник МГАДА. Серия «Экономика», 2013. — № 1 (20). — С. 7–13.

184. Амербаев В. М., Соловьев Р. А., Стемпковский А. Л. Вычислительный элемент модулярной арифметики. Патент на полезную модель № 123995, приоритет от 28.06.2012, зарегистрирован 10.01.2013.
185. Амербаев В. М., Стемпковский А. Л., Соловьев Р. А. Принципы рекурсивных модулярных вычислений // Информационные технологии, 2013. — № 2. — С. 22–27.
186. Амербаев В. М., Тельпухов Д. В. Обратный преобразователь модулярной арифметики с использованием неточного ранга для задач ЦОС // Известия вузов. Электроника, 2013. — № 1. — С. 41–46. Amerbaev V., Stempkovsky A., Solovyev R., Telpukhov D. Efficient Calculation of Cyclic Convolution by Means of Fast Fourier Transform in a Finite Field, Proc. Of 11th East-west design & test symposium (EWDTS 2013).
187. Амербаев В. М., Тельпухов Д. В., Соловьев Р. А. Реализация библиотеки модульных арифметических операций на основе алгоритмов минимизации логических функций // Известия Южного федерального университета. Технические науки, 2013. — № 7 (144). — С. 221–225.
188. Amerbaev Viljan, Soloviev Roman, Telpuhov Dmitriy. Hardware Implementation of FIR Filter Based on Number-Theoretic Fast Fourier Transform in Residue Number System. Open Sciences Journal. 2014. P. 1-6.
189. Stempkovsky A. L., Amerbaev Viljan, Soloviev Roman, Isaeva T. Yu., Balaka E. S., Telpuhov Dmitriy Principles of recursive Residue Number System computation. CEET International conference on Advances in Computing. Electronics and Electrical Technology. Malaysia, Kuala Lumpur. 2014. P. 174–179.
190. Amerbaev V. M., Solovyev R. A., Stempkovskiy A. L., Telpukhov D. V. Efficient calculation of cyclic convolution by means of fast fourier transform in a finite field. Proceedings of IEEE East-West Design and Test Symposium, EWDTS 2014 2014. — P. 7027043.
191. Амербаев В. М. Модулярная арифметика сегодня // История отечественной электронной вычислительной техники. — М.: Столичная энциклопедия, 2014. — С. 199–201.

192. Амербаев В. М., Балака Е. С., Соловьев Р. А., Тельпухов Д. В. Анализ и синтез арифметического узла проф. Поспелова Д. А. поля Галуа // Проблемы разработки перспективных микро- и наноэлектронных систем — 2014 // Сборник научных трудов под общ. ред. А. Л. Стемпковского. — Москва: ИППМ РАН, 2014. — № 4. — С. 179–182.
193. Амербаев В. М., Балака Е. С., Соловьев Р. А., Тельпухов Д. В., Щёлоков А. Н. Применение структурной избыточности для повышения надёжности арифметического узла вычислительного элемента бимодульной арифметики // Известия Южного федерального университета. Технические науки, 2014. — № 7 (156). — С. 255–261.
194. Амербаев В. М., Балака Е. С., Тельпухов Д. В., Соловьев Р. А. Применение информационной избыточности для повышения надежности арифметического узла вычислительного элемента бимодульной арифметики // Параллельная компьютерная алгебра и её приложения в новых инфокоммуникационных системах / Материалы I международной научной конференции. — Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; Институт математики и естественных наук, 2014. — С. 347–358.
195. Амербаев В. М., Балака Е. С., Щёлоков А. Н. Исследование аппаратных методов контроля арифметического узла вычислительного элемента бимодулярной арифметики // Международный конгресс по интеллектуальным системах и информационным технологиям AS-IT 2014.
196. Амербаев В. М., Соловьев Р. А., Тельпухов Д. В. Метод вычисления циклической свертки на базе БПФ с использованием чисел Прота // Информационные технологии, 2014. — № 10. — С. 22–27.
197. Амербаев В. М., Соловьев Р. А., Тельпухов Д. В., Балака Е. С. Построение обратных преобразователей модулярной арифметики с коррекцией ошибок на базе полиадического кода // Нейрокомпьтеры: разработка, применение, 2014. — № 9. — С. 30–35.

198. Амербаев В. М., Соловьев Р. А., Тельпухов Д. В., Балака Е. С. Построение обратных преобразователей модулярной арифметики с коррекцией ошибок на базе полиадического кода // Параллельная компьютерная алгебра и её приложения в новых инфокоммуникационных системах / Материалы I международной научной конференции. Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; Институт математики и естественных наук, 2014. — С. 260–267.
199. Амербаев В. М., Соловьев Р. А., Тельпухов Д. В., Щёлоков А. Н. Исследование эффективности модулярных вычислительных структур при проектировании аппаратных однотактных умножителей // «Известия ЮФУ. Технические науки. — Таганрог, 2014. — № 7 (156). — С. 248–254.
200. Амербаев В. М., Соловьев Р. А., Тельпухов Д. В., Щёлоков А. Н. Исследование и разработка аппаратных однотактных умножителей на базе модулярных вычислительных структур // Международный конгресс по интеллектуальным системах и информационным технологиям AS-IT 2014.
201. Амербаев В. М., Стемпковский А. Л. Принцип факторизации в проблеме проектирования модулярных процессоров // Проблемы разработки перспективных микро- и наноэлектронных систем — 2014 / Сборник научных трудов под общ. ред. А. Л. Стемпковского. — Москва: ИППМ РАН, 2014. — Часть IV. — С. 183–186.
202. Амербаев В. М., Тельпухов Д. В., Соловьев Р. А., Балака Е. С. Разработка аппаратного модулярного фильтра с конечной импульсной характеристикой на базе теоретико-числового быстрого преобразования Фурье // Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем (МЭС)». Сборник трудов, 2014. — № 4. — С. 169–172.
203. Амербаев В. М., Балака Е. С. Вычислительный элемент бимодульной модулярной арифметики. Патент на полезную

модель № 148925, приоритет от 20.03.2014, зарегистрирован 19.11.2014.

204. Абанина И. Н., Амербаев В. М., Бардушкин В. В., Исаченко А. Н., Кожухов И. Б., Костин И. Б., Лесин В. В., Лисовец Ю. П., Митюшкин Р. А., Пиндрикова Л. В., Ревякин А. М., Ревякина М. А., Степанов А. А., Терещенко А. М., Ярошевич В. А. Математические методы принятия решений и модели в управлении и во внешнеэкономической деятельности. — Москва, 2014.
205. Амербаев В. М., Балака Е. С., Тельпухов Д. В., Соловьев Р. А. Применение информационной избыточности для повышения надежности арифметического узла вычислительного элемента бимодульной арифметики // Наука. Инновации. Технологии, 2015. — № 1. — С. 36–50.
206. Амербаев В. М., Соловьев Р. А., Тельпухов Д. В., Поперечный П. С., Рухлов В. С., Щёлоков А. Н., Михмель А. С. Разработка устройства для вычисления результата операции скалярного произведения векторов на базе интрамодулярного разложения комплексных чисел в модулярной арифметике // Известия ЮФУ. Технические науки, 2015. — № 6 (167). — С. 95–105.
207. Амербаев В. М. и др. Полугруппы преобразований, сохраняющие бинарное отношение // Экономические и социально-гуманитарные исследования. — М.: МИЭТ, 2015. — № 4. — С. 17–22.
208. Telpukhov D. V., Solovyev R. A., Amerbaev V. M., Balaka E. S. Hardware implementation of fir filter based on number-theoretic fast fourier transform in residue number system // Проблемы разработки перспективных микро- и наноэлектронных систем (МЭС). 2015. № 4. С. 42.
209. Amerbaev V. M., Balaka E. S., Solovyev R. A., Telpukhov D. V. Analysis and synthesis of arithmetic unit of a field of galois of prof. Pospelov D. A. Проблемы разработки перспективных микро- и наноэлектронных систем (МЭС), 2015. — № 4. — С. 44.

210. Stempkovsky A. L., Amerbaev V. M. The principle of factorization in a problem of design of rns-based processors // Проблемы разработки перспективных микро- и наноэлектронных систем (МЭС), 2015. — № 4. — С. 45.

Это не полный перечень научных трудов В. М. Амербаева, который удалось составить при подготовке книги к выпуску.

Монографии В. М. Амербаева

Всего в библиографии В. М. Амербаева представлено 19 трудов, соответствующих понятию «монография».

Но шесть из них (поз. 39, 46, 51, 52, 53, 119 по библиографии) — отчёты по НИР и ОКР, изданные в нескольких экземплярах, отнесены к категории рукописей. Ещё три (поз. 1, 2 и 12) редакционной группе найти не удалось. Поэтому они в настоящем разделе не рассмотрены.

Десять монографий Вильжана Мавлютиновича общим объёмом 20245 страниц представлены в составе фотографии обложки, предисловия (введения) и оглавления каждой.

1. Акушский И. Я., Амербаев В. М., Пак И. Т. Основы машинной арифметики комплексных чисел. — Алма-Ата: Наука, 1970. — 248 с.

ПРЕДИСЛОВИЕ

Темпы развития науки и техники, глубина и всесторонность проводимых научных исследований приводят к постановке все более сложных задач, решение которых необходимо для народного хозяйства. Оно требует наращивания производительности электронных вычислительных машин. Уже сейчас на 1970–1980 гг. прогнозируется создание вычислительных средств производительностью 10^9 операций в секунду.

Если не касаться вопросов, связанных с разработкой новых методов численного решения задач, программирования

и создания новых машинных языков, то пути дальнейшего совершенствования вычислительных средств просматриваются как в улучшении технико-технологической базы, так и в развитии структуры, логики и организации вычислительных машин.

Первый путь представляет довольно длительный процесс, который включает на начальной стадии открытие физических принципов построения элементов с высоким быстродействием переключения из одного состояния в другое, на следующей стадии — разработку новых эффективных технологических методов (в отношении возможностей массового производства и в экономическом отношении) и, наконец, на завершающей стадии — переоборудование существующих и ввод новых производственных предприятий. Это очень тяжёлый путь, требующий значительного времени и огромных средств.

Вычислительная техника в этом плане прошла уже ряд этапов. С появлением релейной техники чисто механические вычислительные средства перешли в электромеханические. Затем, когда возникла вакуумная электроника, стали строиться ламповые электронные вычислительные машины, которые вместе с радиоэлектроникой совершили переход на полупроводниковую технику. В настоящее время вычислительные средства готовятся сделать следующий шаг — перейти на микроэлектронную технологию и интегральную схемотехнику.

Иное дело второй путь. Он не требует никаких технических и технологических усовершенствований, но зато опирается

на создание новых теоретических концепций в представлении и обработке информации в машине, в построении её структуры и логики и в организации самого процесса решения задач на машинах.

В основе всех методов, создаваемых на этом пути, лежит идея очень простая и в то же время очень сложная — распараллеливание операций. Простая она потому, что естественно возникает, коль скоро одна машина не в состоянии справиться с данным объёмом вычислительных операций и, стало быть, надо привлечь другие машины и распределить работу между ними для одновременного и параллельного её выполнения. Это, в известном смысле, принцип организации любого массового производства, когда различные детали изделия параллельно изготавливаются на различном оборудовании и лишь на заключительной стадии собираются в изделие в окончательном виде. Сложна эта идея тем, что решение далеко не любой задачи может расчленяться на части, допускающие параллельное выполнение на различных машинах. В большинстве случаев алгоритмы решения носят сугубо последовательный характер и только сложными искусственными приёмами удаётся произвести необходимое расчленение, затрачивая при этом значительную часть суммарной производительности машины на осуществление этого расчленения и на последующую увязку всех частей решения между собой. Несмотря на такие весьма существенные трудности в организации параллельной работы различных машин над решением больших задач, создание многомашинных вычислительных систем в настоящее время является важным методом удовлетворения потребностей в высокой производительности.

Весьма перспективно и плодотворно в практическом плане распараллеливание не алгоритмов решения задачи, а распараллеливание на «микроуровне» алгоритмов выполнения элементарных арифметических операций. Здесь понадобилось найти теоретико-числовую основу, определяющую способы разбиения числа на отдельные части, допускающие их независимую и параллельную обработку. Такой основой явилась теория

сравнения. Опираясь на фундаментальные понятия и положения этой теории, удалось построить оригинальную систему счисления в остаточных классах, в которой числа представляются своими вычетами по совокупности взаимно простых модулей — оснований системы и рациональные операции над числами проводятся независимо от соответствующих вычетов этих чисел в отдельности. Система счисления в остаточных классах получила развитие как в теоретическом, так и практическом плане и послужила базой для построения высокопроизводительных вычислительных машин.

Между тем идеи и концепции системы остаточных классов оказались настолько привлекательными, что вызвали стремление расширить сферу их приложения и обобщить их в различных направлениях.

Поскольку в системе остаточных классов отсутствуют явные межразрядные связи, то естественным явилось обобщение в направлении создания общей теории непозиционных систем, которая охватывала бы все возможные системы счисления подобного рода. Такая теория разрабатывается трудами ряда советских учёных и выявила уже весьма интересные системы счисления, обладающие различными специфическими свойствами, важными для эффективной практической реализации.

Другое не менее важное направление — обобщение системы остаточных классов на объекты более сложной природы, чем область вещественных чисел. Работа в этом направлении велась в Институте математики и механики АН КазССР.

Следующей по своей сложности является область комплексных чисел. Построение системы счисления в остаточных классах в комплексной области оказалось возможным на основе гауссовой теории целых комплексных чисел, а гауссова идея изоморфизма между комплексными вычетами числа по комплексному модулю и его вещественными вычетами по норме этого модуля позволила целиком заменить комплексную систему счисления вещественной и тем самым практически создала возможность работать в вещественной области

с комплексными числами в целом без разбиения их на вещественные и комплексные компоненты.

Трудно переоценить то практическое значение, которое имеет эта возможность для решения задач, формируемых в терминах комплексных величин. Алгоритмы решения задач значительно упрощаются, так как в них отсутствует такой элемент, как выделение самостоятельно вещественных и мнимых частей величин и их взаимных связей, а производительность решения задач при этом резко возрастает. Возможность оперировать комплексным числом (или плоским вектором) как элементарным нерасчленяемым объектом сулит интересные перспективы создания новых методов численного решения многих важных задач. В перспективе — перенесение этого метода на пространственные многомерные векторы, а также на элементы некоторых функциональных пространств.

Книга содержит результаты исследований по построению машинной арифметики в комплексной области в охарактеризованном выше направлении.

В первых трёх главах на основе трудов К. Ф. Гаусса по теории биквадратичных вычетов изучены основные вопросы теории делимости, теории сравнений, теории индексов целых комплексных чисел. Особое внимание уделяется анализу понятия полной системы вычетов по комплексным модулям и анализу таблиц модульной арифметики.

Четвертая глава посвящена изучению свойств позиционных систем счисления с комплексными основаниями.

Пятая глава содержит обобщение теории систем счисления остаточных классов на комплексную область и разработку машинных алгоритмов в этих системах счисления. Путём введения специального кодирования рассматриваются способы сокращения таблиц модульного суммирования и умножения. Изучены операции сокращения и расширения диапазона.

Книга представит интерес как для математиков, работающих в области теории математических машин и их применения, так и для инженеров — разработчиков цифровых вычислительных машин, ведущих поиск принципиально новых

путей организации арифметических устройств вычислительных машин и повышения их эффективности.

Авторы выражают глубокую благодарность Э. И. Альзамаровой за оказанную помощь в расчёте таблиц и оформлении рукописи.

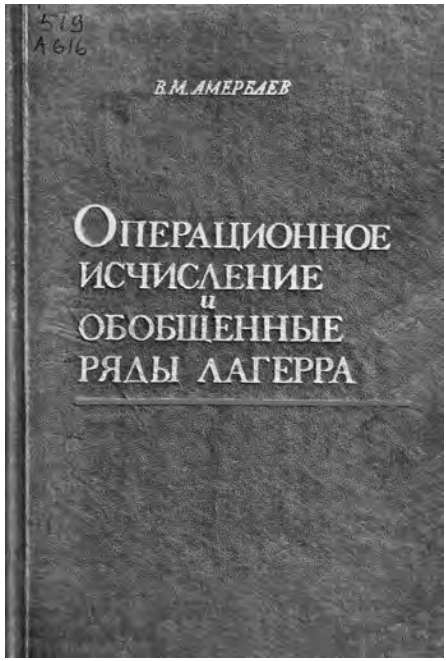
Авторы

ОГЛАВЛЕНИЕ

— • —

2. Амербаев В. М. Операционное исчисление и обобщённые ряды Лагерра. — Алма-Ата: Наука, 1974. — 181 с.

ПРЕДИСЛОВИЕ



Операционное исчисление — важный аппарат современных методов прикладной математики. Самым главным достоинством, обеспечивающим большую популярность этого метода, является алгебраизация основных важнейших линейных процедур математического анализа, что, в свою очередь, открывает большие возможности для «экономики мышления», компактности интерпретаций, широкого использования аппарата алгебры и метода аналогий. Другое не менее важное преимущество его состоит в том, что оно, по существу, служит языком перевода задач теории функций вещественного переменного на язык задач теории функций комплексного переменного, которая обладает развитым и тонким аппаратом.

Развитие теории операционного исчисления стимулировалось тенденцией переноса операционных методов на более общие классы функциональных объектов. Как показывает анализ литературы, проблемой обобщения операционного исчисления занимаются исследователи разных стран. Наиболее широкую известность получили работы Г. Деча, В. А. Диткина, Я. Микусинского, Л. Шварца.

В настоящей книге излагаются элементы нового подхода к построению операционного исчисления. Сущность этого подхода заключается в разработке процедур (типа пополнения пространств), расширяющих область определения операторов. Основу используемого аппарата составляют обобщённые ряды Лагерра и метод аналитического продолжения функций комплексного переменного. Идея метода исходит из эйлеровского обобщения понятия суммы бесконечного ряда. Л. Эйлер писал: «...если под «суммой» ряда понимать, как это обычно делается, результат сложения всех его членов, то нет никакого сомнения, что суммы можно получать только для тех бесконечных рядов, которые являются сходящимися и дают результаты, тем более близкие к некоторому определённому значению, чем больше членов складывается... Мы припишем слову «сумма» значение, отличное от обычного. А именно: мы скажем, что сумма некоторого бесконечного ряда есть конечное выражение, из разложения которого возникает этот ряд» [113].

Последнее предложение является формулировкой знаменитого принципа Эйлера суммирования расходящихся рядов. Эта точка зрения предвосхитила ряд крупных идей последующего развития математики, в том числе идею аналитического продолжения. В частности, сам принцип Эйлера нельзя корректно сформулировать, не используя метода аналитического продолжения.

По Эйлеру, «сумма ряда» является первичным понятием, тогда как «ряд» — производным, вторичным. В обычном понимании картина противоположная: первичным является «ряд», а «сумма ряда» — вторична.

Подобная же схема может быть использована при построении операционного исчисления. В обычном понимании операционного исчисления изображение оригинала $f(t)$ есть функция $F(p)$ комплексного переменного p, получаемая умножением оригинала $f(t)$ на e^{-pt} и интегрированием по t на интервале от 0 до ∞. Следовательно, оригинал является первичным, а изображение — вторичным: оригинал производит изображение.

Аналог эйлеровского принципа в операционном исчислении предполагает такую процедуру построения пространства

изображений, при которой изображение было бы первичным, а оригинал — вторичным: изображение производит оригинал. Последовательно придерживаясь этой точки зрения, можно получить пространство обобщённых оригиналов, где каждый из них понимается как класс эквивалентности во множестве формальных рядов Лагерра. Пространство обобщённых оригиналов изоморфно пространству всех аналитических функций комплексного переменного, которое выступает в роли пространства изображений. Таким образом, в рамках этой теории любая аналитическая функция является изображением, а пространство обобщённых оригиналов выступает как новый тип пространства обобщённых функций. Это пространство в общем случае не является ни полем, ни кольцом, ни линейным пространством. Вместе с тем принцип изоморфного вложения позволяет отождествить отдельные подмножества пространства обобщённых оригиналов с пространством классических функций-оригиналов, с пространством обобщённых функций D_0^+ Л. Шварца, с пространством Я. Микусинского.

В предлагаемой книге приводятся наиболее важные понятия математического анализа и их распространение на обобщённые оригиналы: интегрирование, дифференцирование, свёртка, значение обобщённого оригинала в точках $t = +0$ и $t = +\infty$, обобщение понятия интеграла Лапласа — Карсона на класс обобщённых оригиналов и т. п.

Рассматриваются три стержневые проблемы, возникающие в связи с обобщением операционного исчисления:

1) распространение операционных правил на класс обобщённых оригиналов;

2) изучение состава пространства обобщённых оригиналов, т. е. изучение вопроса о том, какие классы функций принадлежат пространству обобщённых оригиналов и какие (конкретно) изображения им соответствуют;

3) исследование алгоритмов и приёмов построения (реализации) неизвестного оригинала, когда известно изображение.

В связи с небольшим объёмом книги материал, касающийся двух последних проблем, несколько ограничен.

За исключением первой главы, где излагаются элементы дискретного операционного исчисления над произвольным полем, по которым имеется обширная библиография, в книге приводятся библиографические замечания. Цель первой главы — показать идейное (структурное) родство дискретного и непрерывного операционных исчислений, проиллюстрировать на примере дискретных преобразований силу эйлеровских идей по обобщению понятия суммы расходящихся рядов, подготовить идейный фундамент — ввести понятие обобщённого ряда Лагерра для последующего обобщения операционного исчисления.

В начале каждой главы в краткой форме освещаются постановка задачи и содержание.

В книге принята трёхместная нумерация формул (m, n, s): m — глава, n — параграф, s — формула. Ссылки на них внутри параграфа одноместные (s), по главе — двуместные (n, s), по книге — трёхместные (m, n, s).

Автор глубоко благодарен профессорам В. А. Диткину и А. П. Прудникову за неоднократное обсуждение материала и дружескую критику.

В написании книги приняли участие Ж. Наурзбаев, Р. Джаембаев. Ж. Наурзбаевым написан § 3 главы 4, Р. Джаембаевым — § 2, 3 главы 6. Ж. Наурзбаев оказал большую помощь в подготовке библиографического материала. Автор выражает им, а также Э. Альзамаровой свою признательность за помощь в работе над книгой.

ОГЛАВЛЕНИЕ

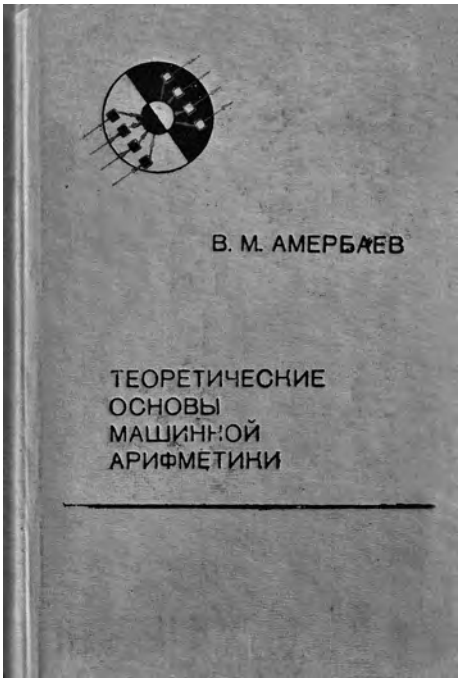
— • —

3. Амербаев В. М. Теоретические основы машинной арифметики. — Алма-Ата: Наука, КазССР, 1976. — 324 с.

ПРЕДИСЛОВИЕ

Прогресс в создании и широком использовании вычислительной техники, в научных исследованиях и народном хозяйстве в немалой степени зависит от решения двух проблем: проектирования вычислительных средств на новой технологической и элементной базе и проектирования систем вычислений на основе широкого привлечения математических конструкций и концепций.

Проектирование систем вычислений как научное направление включает в себя большое число актуальных проблем современной прикладной математики. Отметим две



из них, непосредственно связанные с задачами кодирования.

Первую можно сформулировать следующим образом: разработка системы дискретных аппроксимационных моделей вещественных чисел и математических объектов более сложной природы, чем числа. Логические аспекты её основываются на исследованиях числовых систем и конструктивного анализа и к настоящему времени продвинуты достаточно далеко. Однако вычислительные (операциональные) аспекты этой проблемы разработаны ещё не в полной мере. Имеется в виду конструирование новых дискретных моделей математических объектов, которые бы обеспечивали доступную высокоэффективную (техническую и алгоритмическую) реализацию на них вычислений в рамках того или иного класса задач. В решении этих вопросов главенствующее значение приобретают теоретико-числовые концепции, методы прикладной алгебры, методы конструктивной теории функций и гармонического анализа, включая теорию представлений и характеров, методы вычислительной математики и теории алгоритмов.

В процессах вычислений наблюдается сложное взаимодействие эффектов «двойной» дискретизации: сам вычислительный алгоритм (представляющий, как правило, некую дискретную схему более сложного математического процесса) реализуется не на поле вещественных чисел, как это обычно мысленно полагается при разработке вычислительных алгоритмов, а на

дискретной модели вещественных чисел. Таким образом, вычислительный процесс стратифицируется по меньшей мере в виде двух страт, т. е. в виде взаимодействия модели верхнего уровня (вычислительный алгоритм) с моделью нижнего уровня (дискретная модель вещественных чисел). При решении важных научно-технических задач всё чаще возникают ситуации, когда реализация модели верхнего уровня на фиксированной модели нижнего уровня приводит к процедурным и техническим осложнениям, а порой к изменению качества задачи.

Преодолеть эти трудности можно решением следующих двух взаимосвязанных подпроблем:

- разработать системы аппроксимационных моделей нижнего уровня, обеспечивающие эффективную реализацию на них моделей верхнего уровня (с учётом перспектив развития вычислительной техники);
- согласовать модели верхнего уровня со специфическими требованиями моделей нижнего уровня, вытекающими из задачи эффективной реализации (производительность, надёжность, сохранение качества задачи, экономичность).

Здесь же следует отметить, что прямое и обратное влияние алгоритмической структуры моделей верхнего уровня и арифметической структуры моделей нижнего уровня ввиду значительной ограниченности имеющихся в пользовании дискретных моделей вещественных чисел исследованы ещё не достаточно полно.

Вторая проблема обусловлена процедурами конструктивного именования элементов модели, и сформулировать её можно следующим образом: разработка системы кодирования элементов дискретных моделей верхнего и нижнего уровня в форме, удобной для задач автоматизации и повышения надёжности вычислений (процессов поиска, хранения и обработки информации).

Представляется очевидным тезис, что элементы одной и той же модели могут кодироваться различными системами кодов (имён, обозначений кодовых слов). Важно, чтобы были выполнены следующие требования:

- правила конструирования кодов должны точно фиксироваться и ясно формулироваться;
- соответствие между элементами модели и кодовыми словами, обусловленное правилами конструирования кодов, должно быть изоморфизмом или по меньшей мере корреспонденцией относительно свойств отношений и операций, определённых на модели.

Разработкой таких правил исходя из ограничений, диктуемых состоянием вычислительной техники и её элементной базой, занимается сравнительно молодая ветвь математики — общая теория арифметичного кодирования. Исследования в области кодирования вызваны потребностями практики и влияют на различные стороны технической реализации новых идей, заложенных в конструкции кодов. Поэтому чем шире спектр приёмов кодирования числовых и других математических объектов, участвующих в вычислительных процессах, тем более точным может оказаться решение о конструктивных особенностях проектируемых процессоров, удовлетворяющих заданным требованиям.

Руководящей идеей при построении кодов, обеспечивающих ускорение процессов обработки информации, является идея распараллеливания операций на уровне выполнения элементарных арифметических действий. Влияние указанной идеи заметно сказывается, например, при разработке различных методов ускорения арифметических операций над числами, представленными двоичными кодами; в частности, её реализация здесь приводит к необходимости перехода от традиционного двоичного кодирования к различным модификациям (как то: двоичные коды с основанием –2, двоичные коды с цифрами +1, –1 или +1, О, –1, позиционные коды с дробными основаниями). Цель подобного рода модификаций состоит в том, чтобы сократить число ситуаций, обусловливающих возникновение сквозного переноса в схемах суммирования. Наличие сквозного переноса является существенной характеристикой позиционных кодов. Радикальный отказ от кодов, порождающих сквозной перенос при аддитивных операциях, приводит к кодам с параллельной структурой или иначе к непозиционным

кодам. Параллельная структура кодов позволяет ставить и решать новые задачи, недоступные для позиционных кодов, такие как, например, построение в пределах одного процессора живучих арифметических структур.

Поиск новых форм кодирования арифметических объектов породил широкий фронт исследований. Ситуация в области разработки арифметических кодов к настоящему времени такова. С одной стороны, методы двоичного кодирования изучены достаточно полно и машинная арифметика двоичных кодов приобрела формы классической дисциплины с установившимися канонами и структурой, при этом наблюдается спад «потока новых идей, относящихся к методам выполнения арифметических операций и построение арифметических устройств цифровых вычислительных машин» [30]. С другой стороны, повышение требований, предъявляемых к помехозащищённости и быстродействию, стимулирует интенсивный поиск новых форм кодирования, а следовательно, и новых форм реализации арифметических операций.

В связи с изложенным представляется важным и актуальным изучение вопросов синтеза арифметических кодов в наиболее общей постановке, которые имеют целью исследование фундаментальных принципов и свойств математического аппарата теории арифметического кодирования, а также разработка приёмов повышения быстродействия вычислительных средств на основе анализа различных конструкций арифметических кодов, в первую очередь посредством распараллеливания алгоритмов выполнения операций. Следует подчеркнуть, что содержательный смысл термина «арифметичный» включает в себя как частный случай содержание, вкладываемое в термин «арифметический». Арифметическое кодирование есть кодирование чисел, тогда как арифметичное кодирование подразумевает кодирование более сложных алгебраических объектов (в каждом отдельном случае конкретных), позволяющее обеспечить эффективную техническую и алгоритмическую реализацию соответствующих (алгебраических) операций над указанными элементами.

Все эти частные проблемы проектирования систем вычислений тесно взаимодействуют между собой и составляют ядро

машинной арифметики. Термин «машинная арифметика» укоренился после первых разработок вычислительных средств с автоматическим управлением процесса вычислений. С развитием вычислительной техники семантика этого термина углубляется и расширяется. В настоящее время машинная арифметика находится на перекрёстке важнейших направлений прикладной теории чисел, прикладной алгебры, теории алгебраических систем, теории оценок сложности реализаций (реализаций вычислений на заданной вычислительной структуре, реализаций операций на заданном комплекте элементарных функциональных преобразователей и т. п.), теории оценок точности вычислений и организации вычислительного процесса, теории проектирования вычислительных устройств и систем. Наконец, конкретно прикладные импульсы, определяющие прогресс машинной арифметики, задаются состоянием и ограничениями элементно-технологической базы. Так, в последние годы прогресс в микроэлектронике и оптической электронике способствовал созданию плотных и сверхплотных элементарных вычислительных структур, обладающих большим коэффициентом избыточности, что ставит перед машинной арифметикой совершенно новые, отличные от традиционных проблемы эффективного использования избыточности в реализации различного типа математических операций и процессов.

Одним из фундаментальных понятий машинной арифметики является понятие диапазона дискретной модели заданной математической системы. Алгебраическая структура диапазонов определяет конструктивные особенности кодов, изображающих элементы диапазона, которые существенно влияют на способ реализации (алгоритмы) соответствующих алгебраических операций. Последние, в свою очередь, указывают на пути схемной реализации операций. Так возникает концептуальная цепочка: математическая система «S-дискретная модель»: диапазон $\rightarrow$ кодовый, диапазон $\rightarrow$ машинный, диапазон $\rightarrow$ интерпретация результатов на языке математической системы S.

В книге изучаются методологические (в смысле разработки требований и ограничений) вопросы построения дискретных аппроксимационных моделей вещественных чисел

и математических моделей более общей природы, чем числа; рассматриваются вопросы кодирования элементов конечных дискретных моделей; большое внимание уделяется кодам с параллельной структурой (непозиционным арифметичным кодам), при этом акцент делается на анализ вопросов повышения эффективности реализации так называемых немодульных процедур (с помощью формул неточного ранга, распараллеливания процедуры округления, совершенствования процедур декодирования). Обобщается понятие диапазона на случай кольца главных идеалов, на базе которого строится теория арифметичного кодирования элементов кольца главных идеалов. В качестве частного случая этой теории рассмотрены вопросы арифметичного кодирования функциональных объектов.

В советской и зарубежной литературе имеется ряд работ [31, 33, 36, 40, 60], посвящённых различным аспектам машинной арифметики (в основном вопросам алгоритмической и главным образом схемотехнической реализации арифметических операций над числами, представленными двоичными или другими позиционными кодами). Теоретический же анализ понятия диапазона является фундаментальным, а его структура и свойства служат конструктивной основой процедур арифметичного кодирования. Непозиционным системам счисления посвящены работы [1, 44, 60]. Результаты этих исследований дополняются в данной книге разработкой новых алгоритмических приёмов повышения эффективности выполнения немодульных операций.

Следует отметить, что к настоящему времени накопилось множество публикаций (главным образом журнальных), посвящённых различным вопросам теории и приложения непозиционных систем счисления. Автор не имел возможности дать обзор этих работ. В ссылках отражены лишь те из них, которые непосредственно использованы или имеют прямое отношение к излагаемому материалу.

В книге принята сквозная нумерация по главам, параграфам и внутри каждого параграфа. Так, ссылка на п. 3 параграфа 2 главы 4 будет обозначаться как 2.3 внутри главы 4 и как 4.2.3 в других главах. Для удобства чтения в первой главе

конспективно изложены важнейшие математические термины и понятия, применяемые в последующих главах.

Автор выражает глубокую благодарность и признательность проф. И. Я. Акушскому и проф. Д. И. Юдицкому, под влиянием которых развивался его интерес к непозиционным системам счисления, а также Э. И. Альзамаровой за большую помощь при подготовке рукописи к изданию.

ОГЛАВЛЕНИЕ

— • —

4. Амербаев В. М., Васильев В. И., Гуревич И. М., Пак И. Т. Распределение регулярных потоков сообщений в информационных системах. — Алма-Ата: Наука, 1980. — 143 с.

ПРЕДИСЛОВИЕ

Одну из компонент инфраструктуры современного общества составляют разнообразные системы сбора, хранения, передачи и преобразования информации. Ввиду многообразия и сложности проблем, возникающих в процессе разработки, внедрения и развития информационных систем, а также насущной

необходимости обеспечения эффективного функционирования систем высшего уровня возникает потребность в постановке и решении ряда задач по распределению в информационных системах регулярных или детерминированных потоков информации.

В книге поставлена и рассмотрена задача детерминированного временного распределения регулярных потоков в информационных системах. Информация о координатах *n*-мерного объекта периодически или в соответствии с некоторыми фиксированными алгоритмами поступает в один или несколько каналов связи или обработки (аппаратов обслуживания), осуществляющих временное распределение сообщений. Поскольку одновременная передача информации о двух или более координатах невозможна, требуется решить задачу о временном распределении (ВР) информации в канале связи, получить критерии ВР в различных случаях и, используя их, организовать передачу данных оптимальным образом.

В первой главе книги дан краткий обзор методов уплотнения каналов связи, в том числе методов временного распределения. Приведены примеры информационных систем, в которых осуществляется временное уплотнение (распределение) регулярных или детерминированных потоков сообщений. Перечислены типичные задачи распределения регулярных потоков сообщений, возникающие при построении телеметрических и вычислительных систем, а также систем передачи данных. Описан ряд средств временного распределения.

Вторая глава содержит изложение наиболее распространённых способов определения периодов передачи сообщений, базирующихся на известных методах дискретизации непрерывных сообщений. Приведены выражения для определения периодов передачи сообщений, обеспечивающих требуемую точность.

В третьей главе рассматривается ряд методов определения длительностей передачи сообщений. Одни из них основаны на использовании процедуры оптимального квантования непрерывных сообщений, другие учитывают факт использования одного канала связи для передачи сообщений от нескольких источников информации. С использованием соотношения неопределённости в виде ограничения определены оптимальные точности и, тем самым, длительности передачи при степенном и квадратичном критериях потерь.

Четвёртая глава посвящена изложению методов анализа и распределения детерминированных (главным образом периодических) потоков сообщений.

В пятой главе изложен аппарат исследования задач распределения в канале связи смешанных (детерминированных и стохастических) потоков сообщений. Приведены условия стационарности и выражения для определения вектора состояний системы. Даны оценки максимальной и средней очередей, имитационная модель и результаты статистического моделирования. В подготовке материалов данной главы принимал участие М. А. Медриш.

Шестая глава содержит примеры использования изложенных в книге методов детерминированного распределения для расчёта ряда характеристик информационных систем. Даны выражения для определения параметров каналов связи (пропускной способности, полосы пропускания, мощности полезного сигнала). Изложена задача оптимального выбора длительностей передачи сообщений. Рассмотрена методика оптимального выбора способов использования средств передачи и обработки информации.

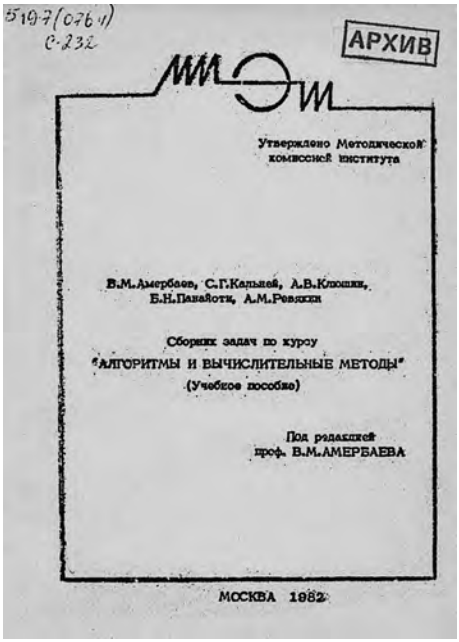
ОГЛАВЛЕНИЕ

— • —

5. Амербаев В. М., Кальней А. Г., Клюшин А. В., Понайоти Б. Н., Ревякин А. М. Сборник задач по курсу «Алгоритмы и вычислительные методы: Учебное пособие. — М.: МИЭТ, 1982. — 118 с.

ВВЕДЕНИЕ

Предлагаемое пособие (первая часть) по полугодовому курсу «Алгоритмы и вычислительные методы» предназначено для студентов, специализирующихся в области проектирования и разработки вычислительных и программных средств, систем автоматизированного проектирования и др. Оно призвано помочь студентам усвоить некоторые важные фундаментальные понятия и методы, используемые в теории вычислений, теории



программирования, вычислительной математике, а преподавателям, ведущим практические занятия, — облегчить подборку задач.

Особенность сборника состоит в том, что в нём рассматриваются важнейшие разделы дискретной математики, использующиеся в анализе и синтезе вычислительных устройств и вычислительных процессов (как числовых, так и нечисловых). Это обусловлено тем, что основные численные методы (интерполирование и аппроксимация функций, численное дифференцирование и интегрирование, разностные методы решения дифференциальных уравнений) нашли отражение в курсе математического анализа, а вводный курс в дискретную математику отсутствует.

В сборнике параграфы 1–3 посвящены стандартным приёмам формализации, составляющим основу языка математического описания объектов, их свойств и отношений между ними. Вместе с тем этот материал является подготовительным для введения понятия «алгебраические структуры». В настоящее время оно прочно вошло в обиход общей теории систем, теории универсальных микропроцессорных секций, программирования вообще и микропрограммирования в частности, теории формализованных систем и т. п. Отдельные алгебраические структуры нашли широкое применение в теории конечных машин (полугруппы), теории кодирования (группы, конечные поля, кольца полиномов) и т. п. Графы и алгоритмы на графах

(метод ветвей и границ) являются универсальным средством современного инженера, помогающим формулировать и решать многие практические задачи дискретной природы.

Последние параграфы касаются машинных методов вычислений. Здесь обращается внимание на необходимость строгого анализа накопления ошибок в условиях массовых автоматических вычислений с фиксированной разрядностью машинного диапазона. Особенности накопления ошибок иллюстрируются задачами линейной алгебры.

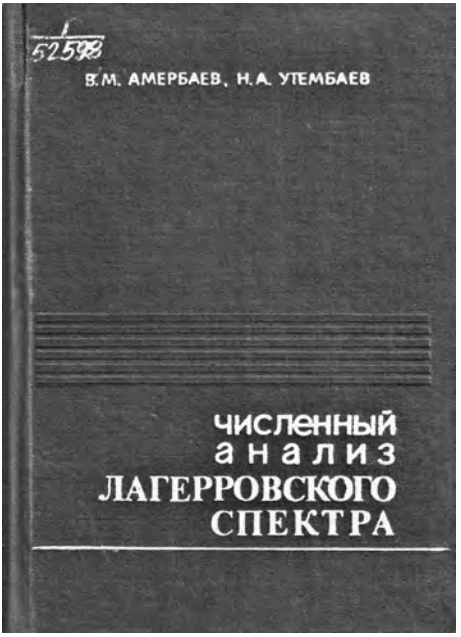
Таким образом, сведения, изложенные в пособии, могут оказаться полезными как при изучении специальных курсов, так и при знакомстве с современной литературой по теории машин и программированию, теории формальных грамматик и т. п.

Авторы выражают благодарность О. К. Загребаловой и Т. А. Хван за большую работу по оформлению рукописи.

ОГЛАВЛЕНИЕ

— • —

6. Амербаев В. М., Утембаев Н. А. Численный анализ лагерровского спектра. — Алма-Ата: Наука, 1982. — 186 с.



Операционное исчисление — важный аппарат современных методов прикладной математики. Самым главным достоинством, обеспечивающим популярность этого метода, является алгебраизация основных линейных процедур математического анализа, что, в свою очередь, открывает большие возможности для «экономии мышления», компактности интерпретаций, широкого использования аппарата алгебры и метода аналогий. Другое, не менее важное его преимущество состоит в том, что оно, по существу, служит языком перевода задач теории функций вещественного переменного на язык теории функций комплексного переменного, которая обладает совершенным и тонким аппаратом.

Развитие теории операционного исчисления стимулировалось тенденцией переноса операционных методов на более общие классы функциональных объектов. Как показывает анализ литературы, проблемой обобщения операционного исчисления занимаются исследователи разных стран. Наиболее широкую известность получили работы Г. Дёча, В. Диткина, Я. Микусинского, Л. Шварца.

При решении задач прикладной математики, механики наибольшее признание получили операционные методы, основанные на интегральном преобразовании Лапласа, с помощью

которого эффективно решаются многие функциональные уравнения, такие как дифференциальные (обыкновенные и в частных производных), интегральные, разностные и другие.

Как правило, при решении подобных уравнений операционными методами основной доли затрат труда, а часто и большей изобретательности требует процесс обращения, т. е. возврат от функции-изображения к искомой функции-оригиналу. Созданы таблицы соответствий, во многих случаях облегчающие и ускоряющие решение задачи обращения. В отечественной литературе наибольшее распространение получили справочники В. А. Диткина, П. И. Кузнецова [31], В. А. Диткина, А. П. Прудникова [30].

Существует ряд приёмов, носящих название «теорем разложения», которые позволяют в некоторых случаях находить точно или приближённо значение искомой функции-оригинала по заданному изображению.

Наконец, наиболее мощным орудием обращения преобразования Лапласа является интегральная формула обращения Меллина — Римана, привлекающая к решению вопросов обращения аппарат теории контурного интегрирования.

Тем не менее широкое применение операционных методов на практике приводит порой к таким функциям-изображениям, к которым в силу ряда причин не могут быть применены приёмы обращения, в отличие от упомянутых выше и ставших уже классическими.

Отметим ряд обстоятельств, когда применение точных приёмов обращения интегрального преобразования Лапласа невозможно или нецелесообразно:

- неизвестен явный аналитический вид функции-изображения. Это может случиться, когда «изображённое» уравнение оказывается неразрешимым в точном виде относительно функции-изображения искомого оригинала или когда функция-изображение искомого оригинала содержит в качестве составной (нелинейной) части функцию-изображение, явный вид которой неизвестен;
- явный вид функции-изображения известен, однако это изображение имеет громоздкую форму, малодоступную

для применения контурного интегрирования или какого-либо другого приёма обращения из-за сложности полного анализа всех особенностей функции-изображения;

- наконец, случай, когда по заданному изображению можно точно восстановить оригинал, однако последний имеет громоздкую аналитическую форму, создающую препятствия для непосредственного числового обозрения полученной функции.

В связи с этим возникает задача построения численных методов, приближенно восстанавливающих функцию-оригинал по заданному изображению. В общем случае поставленную задачу следует понимать как построение некоторых численных приёмов решения интегрального уравнения Фредгольма первого рода с бесконечными пределами интегрирования:

$$\int_0^\infty e^{-pt} f(t)dt = F(p). \qquad (1)$$

Поскольку равенство (1) справедливо лишь для $\mathrm{Re}\, p \geq \gamma \geq \gamma_a$ (где γ_a — абсцисса сходимости интеграла Лапласа), то для приближенного решения такого уравнения естественно использовать информацию, которую содержит в себе числовое значение функции $P(p)$ в точках p полуплоскости $\mathrm{Re}\, p \geq \gamma$.

Такой подход позволяет полностью отвлечься от всех особых точек функции-изображения $P(p)$, расположенных в полуплоскости $\mathrm{Re}\, p \geq \gamma$ (полюсы, существенно особые точки, точки ветвления). Это, в свою очередь, позволит придать вычислительному процессу более универсальный характер, не зависящий от частных характеристик рассматриваемой функции-изображения, в отличие от точных приёмов обращения, основанных на контурном интегрировании, которые существенно опираются на полный анализ всех особенностей функции-изображения. Следует отметить, что этот подход наиболее полно соответствует характеру причин, приводящих к необходимости построения приближенных формул обращения.

Однако построение численных алгоритмов для решения проблемы обращения сталкивается с одной из серьёзных трудностей — с неустойчивостью оригинала относительно малых

изменений изображения. Следовательно, задача обращения преобразования Лапласа согласно [69] относится к классу некорректных задач. Эта особенность делает многие приёмы численного обращения преобразования Лапласа малопригодными для практического использования. Трудности связаны в основном с тем, что при решении проблемы обращения оставляют без внимания или некритически применяют стандартные методы регуляризации, разработанные для общего случая операторных уравнений, которые не учитывают специфики рассматриваемого интегрального уравнения.

В предлагаемой вниманию читателя книге рассматриваются методы восстановления оригинала посредством ортогональных рядов Лагерра, использование которых обусловлено тем, что изображение многочленов Лагерра конформным отображением расширенной плоскости на себя сводится к степенной функции. Этот факт лежит в основе многих исследований рядов Лагерра. В свою очередь, связь степенных рядов с тригонометрическими позволяет применить для решения проблемы обращения мощные методы гармонического анализа, обладающие богатым арсеналом методов улучшения сходимости, оценки приближений, методов определения коэффициентов разложения (в частности, методами быстрого преобразования Фурье (БПФ)), методами устойчивого суммирования.

Первая глава посвящена вопросам связи рядов Лагерра с достаточно широким классом интегральных преобразований, имеющих большое теоретическое и прикладное значение. Часть полученных здесь разложений представляет интерес для теории специальных функций. Во второй главе исследуются алгоритмы и приёмы построения неизвестного оригинала по заданному изображению на базе методов гармонического анализа и устойчивого суммирования рядов Лагерра. Третья глава посвящена некоторым приложениям лагерровского спектра для решения конкретных практических задач. В заключение приводится обзор современного состояния проблемы численного обращения преобразования Лапласа.

ОГЛАВЛЕНИЕ

— • —

7. Амербаев В. М., Пак И. Т. Параллельные вычисления в комплексной плосткости. — Алма-Ата: Наука, 1970. — 182 с.

ПРЕДИСЛОВИЕ

Уровень развития современной микроэлектроники (микропроцессоры, БИС, СБИС и т. д.) открывает перед разработчиками вычислительных средств большие потенциальные возможности в выборе архитектурных и арифметико-логических решений.

Широкое применение в разработках современных вычислительных средств получили методы, направленные на повышение эффективности (производительность, помехоустойчивость, отказоустойчивость, прогнозируемость состояний, диагностируемость

неисправностей и пр.), что достигается средствами специального кодирования. Теория арифметического кодирования, интенсивно развиваемая в последние десятилетия, внедряется в разработках приёмов кодирования числовых и других математических объектов, участвующих в вычислительных процессах.

Мало изучены до сих пор вопросы представления комплекснозначной информации в информационных процессах. Традиционное использование комплексных чисел посредством выделения в них действительной и мнимой частей, т. е. в координатной форме, не даёт необходимого повышения эффективности и надёжности вычислительных процессов. Между тем комплексные числа как математические объекты имеют свою внутреннюю структуру, не зависящую от координатного представления. На это обратил внимание ещё Гаусс [12].

В монографии [2] впервые были изучены комплексные числа с точки зрения вычислительных аспектов. Принятая в ней бескоординатная форма представления комплексных чисел позволяет разработать такую систему кодовой записи, в результате которой удаётся значительно повысить скорость выполнения элементарных операций над комплексными числами.

Исследованию специфичных вопросов кодирования комплексных чисел, способов машинной реализации, анализу различных аспектов применения разрабатываемой теории для повышения эффективности обработки комплекснозначной информации посвящена настоящая монография.

В ней представлены результаты многолетней работы авторов по созданию теории и практики эффективного кодирования комплексной информации, которые являются обобщением и продолжением исследований [2].

Под эффективностью кодирования комплексной информации понимается такая особенность кодирования комплексных величин, которая позволяет:

- во-первых, так организовать вычисления в поле комплексных чисел, что создаются выигрыш временных затрат, экономия ёмкостей оперативных запоминающих устройств и надёжность вычислений при заданных ограничениях на точность вычислений,
- во-вторых, открывается возможность применения предложенных кодов для хранения, передачи и обработки большого потока планарной информации, чтобы обеспечить основы построения регулярных методов создания реконфигурационной арифметики и на этой основе повысить процент выхода годных БИС арифметических процессоров на кристаллах.

На наш взгляд, актуальность, научная и практическая ценность поднимаемых вопросов и предлагаемых решений несомненна. Книга также может оказать содействие внедрению новой перспективной вычислительной идеологии в проектировании специализированных вычислительных средств.

Монография состоит из двух частей.

Первая часть (три главы) посвящена разработке теории и методов модулярной арифметики комплексных чисел. Здесь изучаются вопросы градуирования и шкалирования комплексных величин, понятие машинного диапазона; распространяются на комплексные числа режимы вычислений с фиксированной и плавающей запятой; излагаются основы теории сравнений целых комплексных чисел (гауссовых чисел); раскрывается алгебраическая структура машинного диапазона; показано, что поскольку комплексные числа не наделены отношением порядка (подобно вещественным числам), то преимущества позиционного кодирования комплексных чисел ослабляются. Вместе с тем авторы считают, что приведённые здесь анализы

принципов позиционного кодирования комплексных чисел оригинальны и представляют самостоятельный интерес для теории и практики вычислений комплексных чисел.

Детально рассматривается модулярная арифметика комплексных чисел, в которой достигнута существенная эффективность машинной реализации алгоритмов немодульных операций благодаря использованию попарно взаимно простых комплексно-сопряжённых оснований. Дано определение гауссовой арифметики как арифметики кольца вычетов гауссовых чисел по составному модулю, состоящего из попарно взаимно простых комплексно-сопряжённых целых гауссовых чисел. Все вычислительные процедуры в этой арифметике реализуются в классе вещественных вычетов по вещественным модулям.

Многие из рассматриваемых нами вопросов впервые поднимаются в научно-технической литературе. Используя операторы Ц(•) и д(•), мы выработали единые идейные позиции при анализе и синтезе вычислительных (кодонезависимых) и машинных (кодозависимых) аспектов реализации алгоритмов.

Вторая часть книги (четвертая глава) посвящена новым интересным приложениям гауссовой арифметики. Показано, что в гауссовой арифметике эффективно распараллеливаются вычислительные процедуры, связанные с решением многих практических задач. В частности, при специальном выборе оснований она распараллеливает теоретико-числовое быстрое преобразование Фурье, что существенно ускоряет процесс вычисления свёрток и корреляционных функций и обеспечивает гарантированную точность вычислений.

Рассмотрены два варианта распараллеливания БПФ тригонометрического базиса в гауссовой арифметике, основанных на представлении ДПФ в виде циклических свёрток. Показано, что фундаментальные операции линейной алгебры: скалярное произведение векторов, умножение матриц на вектор, умножение матрицы на матрицу — представляют класс процедур, допускающих эффективную реализацию в гауссовой арифметике. Большая эффективность достигается в гауссовой арифметике при решении алгебраических систем высокого порядка итерационными методами.

Авторы надеются, что книга представит интерес для специалистов, работающих в областях как теории обработки информации, так и разработки специализированных вычислительных структур.

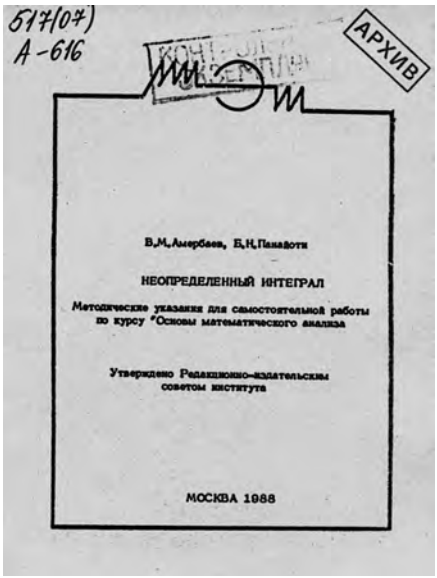
Авторы

ОГЛАВЛЕНИЕ

— • —

8. Амербаев В. М., Понайоти Б. Н. Неопределённый интеграл. Методические указания для самостоятельной работы по курсу «Основы математического анализа. — М.: МИЭТ, 1988. — 28 с.

ВВЕДЕНИЕ



Методические указания предназначены для студентов 1-го курса факультетов МП и ТК и ЭМ, они также могут быть использованы при изучении курса математического анализа и студентами других факультетов. Техника интегрирования необходима для усвоения курса математического анализа и специальных дисциплин. Важным фактором приобретения необходимых навыков интегрирования является самостоятельная работа студентов. В учебной литературе техника интегрирования изложена весьма широко, что часто затрудняет выбор необходимого материала.

Настоящие методические указания должны помочь студенту усвоить необходимый минимум знаний о методах интегрирования и приобрести соответствующие навыки.

ОГЛАВЛЕНИЕ

— • —

9. Амербаев В. М., Ашимов А. А., Сарыпбеков Ж. С. Информатизация республики: концепции и проблемы [Аналитический обзор]. — Алма-Ата: КазНИИНТИ, 1991. — 88 с.

УДК 681.3 Р 50.01.11

Информатизация республики: концепции и проблемы / В.М.Амербаев А.А.Ашимов, Ж.С.Сарыпбеков. – Алма-Ата: КазНИИНКИ, 1991.

Обзор посвящен анализу современного состояния информатизации различных сфер человеческой деятельности, концепции и проблем создания информационной инфраструктуры на основе методов и средств новой информационной технологии (НИТ). Подробно рассматривается роль информатизации в интенсификации социально-экономического развития страны и республики. Дается общая модель информатизации республики, которая позволит комплексно описать основные принципы и концептуальные решения проблем создания систем искусственного интеллекта и автоматизированных систем проектирования, исследований, управления, планирования, обучения и др. Описываются ключевые информационные сферы внедрения НИТ, пути достижения цели, этапы и контрольные цифры развития информатизации республики и оценка эффективности.

Обзор предназначен для широкого круга специалистов и руководителей различных сфер деятельности, инженерно-технических работников в области информатики и вычислительной техники.

Библиогр. 32 назв. Ил. 7. Табл. 9.

Госкомитет Казахской ССР по экономике

Казахский научно-исследовательский институт
научно-технической и конъюнктурно-коммерческой информации
с вычислительным центром

В.М.Амербаев, А.А.Ашимов, Ж.С.Сарыпбеков

ИНФОРМАТИЗАЦИЯ РЕСПУБЛИКИ: КОНЦЕПЦИИ И ПРОБЛЕМЫ

ВВЕДЕНИЕ

Характерной особенностью последней четверти XX в. является так называемый "информационный взрыв", характеризуемый тем, что время удвоения объема общечеловеческих (общеобразовательных) и специальных (профессиональных) знаний составляет 2...3 года. Эти знания, в свою очередь, обеспечивали новое качественное социально-экономическое развитие современного общества путем непрерывного совершенствования механизмов управления отраслями экономики, интенсификации производства, расширения и обновления номенклатуры выпускаемой продукции, товаров, услуг и т.д.

Резкие темпы роста информационных потоков обусловили то, что, по данным ЮНЕСКО, более половины занятого населения наиболее развитых стран принимает непосредственное участие в процессах производства и распространения информации, а в ряде стран до половины национального продукта связано с информационной деятельностью общества. Например, изучение векового процесса перераспределения трудовых ресурсов из сферы материального производства и об-

служивания в информационную сферу экономики США показывает, что к 2000 г. около 75...80 % трудового населения США будут заняты информационной сферой.

Этот информационный взрыв был вызван феноменальным по масштабу и скорости научно-техническим прогрессом в области компьютерной техники и средств передачи данных, самоускорением этого процесса и вызванным этим прогрессом новым глобальным социальным процессом информатизации общества путем массового внедрения в жизнь общества новых информационных технологий.

Массовое использование информационных технологий в промышленно развитых странах приводит к сдвигам в характере и качестве общественного труда. Доминантой становится сфера информационных услуг, оттесняющая на второй план сферу материального производства.

Итогом столь радикальных преобразований, вызванных процессом информатизации, должно стать создание информационного общества. Важной особенностью такого общества будет доступность для каждого его члена всей совокупности общезначимых знаний в требуемое время, нужном месте, необходимом количестве и нужной форме.

Степень обеспеченности оперативной информацией руководителей, ученых и специалистов является одним из основных факторов роста производительности труда и повышения благосостояния народа. Поэтому в индустриально развитых странах важное значение придавалось и придается осмыслению глобального процесса информатизации общества в виде концепции на правительственном уровне, развитию информационной инфраструктуры на основе национальных программ и информация в этих странах стала рассматриваться одной из важных национальных ресурсов.

Таким образом, информатизация общества – это глобальный социальный процесс создания и повсеместного использования информационных ресурсов во всех сферах деятельности общества. Она обеспечивает интенсификацию экономики, ускорение научно-технического процесса страны, процессов демократизации и интеллектуализации общества. Информатизация предусматривает массовое внедрение средств сбора, обработки, передачи и хранения средств информации вычисли-

тельной техники (СВТ) и средств передачи информации, внедрение новых информационных технологий (НИТ).

Сложившееся в целом в СССР состояние дел в вопросах информатизации можно оценить как критическое, а в республике – катастрофическое. Отставание Советского Союза от развитых и даже развивающихся стран по целому ряду параметров может быть оценено интервалом в 10...20 лет. Республика же отстает от союзного уровня еще на десять лет. Имея крайне малое инвестирование в сферу информатики, в республике имеющимися средствами распоряжались нецеленаправленно, без получения адекватной отдачи от использования средств ВТ.

В республике протокольным решением Комиссии Президиума Совета Министров Казахской ССР создана рабочая группа по разработке концепции и программы информатизации республики. Рабочая группа с учетом региональных особенностей, задач социально-экономического развития и предложенных версий концепции информатизации общества в стране разработала концепцию информатизации республики, которая утверждена решением Президиума Совета Министров Казахской ССР от 4 сентября 1990 г. № 21-УШ /1/. Рабочей группой подготовлен проект программы информатизации Казахской ССР в 1991-1995 гг. и на период до 2005 года / 2 /.

В аналитическом обзоре на основе сравнительного анализа различных подходов к решению проблем информатизации в СССР и за рубежом /3...12/ рассматриваются региональные особенности, основные принципы, концепции и проблемы информатизации Казахской ССР. Особое место в обзоре занимает рассмотрение основных направлений информатизации, создание инфраструктуры информатизации республики, разработка и широкое применение методов и средств новой информационной технологии в различных сферах деятельности общества.

Главной задачей обзора является доведение в доступной форме до широкой аудитории заинтересованных лиц, управленческих и научно-технических работников основных положений и проблем информатизации, путей их решения, этапов

развития и контрольных цифр оценки эффективности информатизации республики так, чтобы каждый из них убедился в необходимости и важности данного направления в социально-экономическом развитии республики. При этом члены рабочей группы, в том числе авторы данного обзора надеются, что информатизация не встанет в печальный и трагический ряд: индустриализация – коллективизация – химизация – информатизация. Кроме того, нельзя допустить, чтобы информатизация реализовывалась теми же методами и средствами, которыми реализовывались последние государственные программы об энергетике, продовольствии и т.д.

ПРОБЛЕМЫ ИНФОРМАТИЗАЦИИ РЕСПУБЛИКИ

Анализ состояния информационной инфраструктуры республики

В процессе разработки проекта концепции информатизации республики учтен ряд важнейших особенностей социально-экономического развития и уровня информационной инфраструктуры народного хозяйства Казахстана / 13, 14 /. К таким региональ м особенностям республики можно отнести следующие:

– экономика республики носит ярко выраженный сырье-придаточный характер (в структуре вывоза продукции 70 % составляет сырье, 12 % – полуфабрикаты, а объем ввоза готовой продукции в денежном выражении превышает вывоз примерно в 2 раза);

– среди всех союзных республик Казахская ССР имеет самый низкий удельный вес наукоемких и высокорентабельных отраслей народного хозяйства;

– насыщение народного хозяйства новой техникой в республике идет в основном за счет техники, создаваемой в других регионах страны. Например, доля Казахстана в создании новой техники в общем ее объеме, создаваемой и осваиваемой в стране, составила в 9-й пятилетке 1,37 %, 10-й – 0,9 и в 11-й – 0,6 %. Также низки на предприяти-

ях республики темпы обновления продукции;

– в связи с негативными особенностями социально-экономического развития республики в "Схеме развития и размещения производительных сил Казахской ССР до 2005 года "предусмотрены меры по усилению роли интенсивных факторов экономического роста, совершенствованию структуры народного хозяйства и промышленности и обеспечению полного сбалансирования произведенного и используемого национального дохода к 2000 году. При этом объем промышленного производства за 1991–2005 гг. возрастет в 2,4 раза, за счет повышения производительности труда в 2,6 раза, фондоотдачи на 28 % и снижения материалоемкости на 7,7 пункта. Успешное устранение негативных особенностей и решение задач социально-экономического развития республики в условиях преобразования социально-экономических отношений и демократизации общественной жизни невозможно без создания информационной среды, необходимой для решения всего комплекса важнейших задач экономического, социального и научно-технического развития республики;

– по уровню развития информационной инфраструктуры народного хозяйства республика в настоящее время занимает одно из последних мест среди союзных республик. Так, например, Казахстан по удельному весу междугородних телефонных каналов на связях, оборудованных аппаратурой автоматики и полуавтоматики, занимает 11-е место среди союзных республик, а по числу телефонных аппаратов общего пользования на 100 человек – 9-е место. Слабый уровень информационной инфраструктуры народного хозяйства республики объясняется рядом факторов, в частности:

– недостаточным вниманием к процессу информатизации – одному из главных направлений современной научно-технической революции, важнейшему фактору развития современного общества;

– практическим отсутствием промышленной базы по производству средств вычислительной техники, передачи данных и других технических средств информатизации;

– низким уровнем развития фундаментальных и прикладных

исследований в области информатики; анализ внедрения и и и

– отсутствием экономического механизма создания и развития единой информационной инфраструктуры народного хозяйства республики;

– неподготовленностью республики к информатизации в социальном, экономическом и психологическом плане.

Знание и информационные технологии плохо осознаются в качестве важного ресурса для решения накопившихся социальных и экономических проблем республики. Необходимость информатизации, выделение для этого достаточно больших средств не является очевидным для общества, хотя интуитивно понимается важность этого процесса для решения стоящих перед республикой задач ее развития.

В настоящее время в республике процесс информатизации осуществляется в рамках республиканской программы Р.О.77.01 "Создания, развития автоматизированных систем и эффективного использования вычислительной техники в министерствах и ведомствах Казахской ССР на 1986–1990 гг. и на период до 2000 года", принятой в рамках Общегосударственной программы.

Основой технического обеспечения разрабатываемых и развиваемых автоматизированных систем различных назначений в Казахской ССР является парк ЭВМ республики, насчитывающей около 3500 ЭВМ, в том числе: более 430 вычислительных комплексов на базе процессоров общего назначения, свыше 570 управляющих и вычислительных комплексов на базе минипроцессоров и более 2500 персональных и микроЭВМ, поставленных из других регионов страны. Более 50 % парка ЭВМ на базе процессоров общего назначения составляют устаревшие модели (ЕС–1022, ЕС–1033, ЕС–1035, ЕС–1045, СМ–4, Наири и др.). По своему техническому уровню имеющиеся средства вычислительной техники отстают от аналогичных зарубежных образцов в среднем на 10...20 лет по функциональным показателям (перечню предоставляемых услуг, быстродействию, памяти, материалоемкости, технологичности, надежности, энергопотреблению и насыщенности ЭВМ необходимым периферийным оборудованием, средствами теле-

обработки и средствами репрографии).

Имеющийся парк ЭВМ, являющийся основой функционирования 343 автоматизированных систем, используется неудовлетворительно. Низкая среднесуточная загрузка ЭВМ наблюдается во многих вычислительных центрах министерств и ведомств республики. Отсутствует республиканский фонд алгоритмов и программ.

Современное состояние отрасли связи представляющей традиционные средства информатики (телефон, телевидение, радиовещание и др.), в Казахстане характеризуется низким уровнем удовлетворения потребности народного хозяйства и населения в услугах связи, телевидения и радиовещания, а также более низкими, чем по стране в целом, качественными и количественными показателями их развития. Казахстан имеет серьезное отставание в развитии сети междугородних и зональных каналов связи по сравнению с ростом местных телефонных сетей.

Вместе с тем до настоящего времени отсутствуют надежные методы измерения уровня информатизации. Существующая статистика в виде показателей числа АСУ различного назначения, показателей затрат на их создание не могут служить достоверными критериями оценки эффективности, поэтому проведенный анализ состояния информатизации республики в известной мере опирается на экспертные оценки.

Цели информатизации республики

Цель информатизации Казахской ССР заключается в создании высокоорганизованной информационной инфраструктуры, которая должна способствовать значительному подъему эффективности общественного производства, повышению интеллектуального и культурного потенциала, качества и уровня жизни всего населения республики.

Информатизации республики – это комплекс мер и процессов создания и эффективного использования информационных ресурсов во всех сферах деятельности общества. Главной задачей информатизации республики является своевременное и

качественное информационное обслуживание отраслей экономики и всех общественно значимых сфер человеческой деятельности путем систематической и эффективной реорганизации информационной сферы в целях наиболее полного удовлетворения информационных потребностей общества. При этом информатизация республики должна решить следующие основные задачи:

1) социальную – удовлетворение потребностей человека и повышение его жизненного уровня;

2) организационно-экономическую – повышение эффективности и объемов производства, улучшение качества продукции, индивидуализация товаров;

3) политическую – обеспечение демократии и гласности;

4) культурную – повышение уровня образованности населения;

5) научно-техническую – повышение качества подготовки специалистов, научно-технической компетентности профессиональных работников;

6) психологическую – формирование в республике благоприятного климата в поддержку информатизации;

7) техническую – участие в международном и всесоюзном разделении труда в области разработки и создания средств вычислительной техники и информатики.

Из вышеперечисленных задач наибольшую актуальность представляют социальная, организационно-экономическая и политическая. Поэтому более подробно рассмотрим последствия информатизации республики в этих трех направлениях, которые сводятся:

1) в социальном плане к:

– обеспечение нового качественного уровня здравоохранения за счет широкого использования медицинских приборов, информационных и диагностических систем и устройств, использующих микропроцессорную и вычислительную технику;

– повышению качества образования за счет создания и внедрения компьютерных обучающих систем, специальных систем повышения квалификации;

– повышению уровня жизни народа за счет широкого внедрения систем массового обслуживания, обеспечивающих осу-

ществление на практике принципов социальной справедливости при решении проблем распределения общественных благ;

– осуществлению мониторинга среды обитания с целью оперативного информирования и предупреждения населения;

– развитию новых форм досуга и отдыха населения;

– расширению перечня и повышению качества услуг, предоставляемых населению;

– созданию более комфортных условий труда, его интеллектуализации с целью более полного раскрытия творческих способностей трудящихся;

2) в организационно-экономическом плане к:

– обеспечению структурного преобразования сферы материального производства на основе развития наукоемких отраслей, внедрению ресурсосберегающих технологий;

– ускорению научно-технического прогресса, сокращению сроков и повышению уровня научных исследований и проектно-конструкторских работ;

– интенсификации производства на основе использования в технологическом оборудовании средств микропроцессорной техники;

– моделированию последствий крупномасштабных социальных и экономических проектов до их реализации, реализации современных методов управления и прогнозирования на основе внедрения новых информационных технологий и систем принятия решений;

3) в политическом плане к:

– созданию необходимых условий для доступа широких масс к информации;

– обеспечению возможности рационального сочетания принципов самоуправления и самофинансирования республики в целом, областей, городов и районов в интересах страны, республики и ее отдельных регионов;

– укреплению политических институтов общества за счет информационных технологий в вопросах демократизации и гласности, сближению и консолидации людей, снижению напряженности в межнациональных и других социальных отношениях.

Информатизация является необходимым научно-техническим прорывом в будущее. На это пошли все развитые страны, придав информатизации высшие приоритеты, подчинив этой цели основные ресурсы и усилия.

Владение информацией – это владение экономической и политической властью. Владение информацией невозможно без владения или свободного доступа к средствам и методам ее обработки, передачи и использования. Следует четко осознавать, что информатизация – глобальный фактор экономического суверенитета республики.

ОСНОВНЫЕ ПРИНЦИПЫ ИНФОРМАТИЗАЦИИ РЕСПУБЛИКИ

Учитывая региональные особенности развития экономики и состояние применения вычислительной техники в республике, целесообразно информатизацию осуществлять, исходя из следующих принципов.

Принцип согласования с другими программами социально-экономического развития Казахской ССР означает взаимообусловленность и сбалансированность развития информатизации с развитием всего народного хозяйства республики.

Принцип саморазвития и самофинансирования означает, что процесс информатизации должен воспроизводиться в расширенном масштабе за счет формирования все новых информационных процессов и потребностей, обеспечения сомоокупаемости информатики, как отрасли. Информатизация не должна предстать в виде "посаженной" на экономику республики дополнительной нагрузки и составлять конкуренцию другим насущным программам. Не исключая централизованное финансирование для решения ряда вопросов следует подчеркнуть, что информатизация республики должна в основном строиться на собственных ресурсах. Централизованное финансирование в виде госзаказа и централизованных капитальных вложений направляются на достижение стратегических целей информатизации (например: инфраструктура, база знаний и т.д.). Прик-

ладные аспекты информатизации реализуются за счет средств государственных, кооперативных и смешанных предприятий, привлечения финансовых ресурсов министерств и областных бюджетов.

Принцип самоуправления означает выработку и реализацию собственной республиканской политики в области информатизации. Его реализация заключается в создании республиканской отрасли по информатизации, четкое разделение прав, обязанностей и функций центра и республики, конкурсное размещение заказов между республиканскими, союзными и союзно-республиканскими предприятиями и организациями, создание системы республиканских стандартов и других требований, обязательных для выполнения всеми предприятиями и организациями, независимо от ведомственной подчиненности.

Вместе с тем предстоит выработать собственную региональную политику в республике. Стратегию информатизации республики надо ориентировать на создание таких отраслей и производств, которые, во-первых, соответствуют собственным возможностям областей республики, во-вторых, способны достойно конкурировать на общесоюзном и внешнем рынках, и, в-третьих, обеспечивать потребности республики, не покрываемые в рамках общественного разделения труда.

Процесс информатизации республики требует активного участия Казахстана в союзном и международном разделении труда. Это определяет необходимость создания научных, учебных и промышленных комплексов, которые должны обеспечивать проведение фундаментальных исследований, сквозную подготовку и переподготовку кадров, строительство новых и создание совместных с зарубежными фирмами предприятий по производству средств ВТ и телекоммуникаций, формирование совместных научно-технических программ со странами СЭВ, обучение студентов, стажировку и подготовку специалистов в зарубежных вузах и научных центрах.

Принцип опережающей подготовки общественности к информатизации должен обеспечиваться путем своевременного и полного удовлетворения информационных потребностей общест-

ва, широкой продажей населению бытовых ПЭВМ и функциональных элементов средств ВТ для развития индивидуального творчества, создания клубов, обучающих центров, игротек и т.п.

В социальном плане – это широкое использование средств информатизации в сфере бытовых услуг и материального производства, создание показательных объектов информатизации, раскрытие и доступность информации, использование средств массовой информации для агитации и рекламы, компьютерное образование для формирования в республике благоприятного психологического климата в восприятии идей информатизации и для формирования социального заказа на информатизацию.

Принцип двуязычия (многоязычия) развития информатики. Информатизация должна благотворным образом повлиять на решение проблемы межнационального общения. Государственное казахско-русское двуязычие и равноправное развитие других языков народов, населяющих многонациональную республику, требуют решения следующих проблем информатизации:

– организации на предприятиях республики выпуска клавиатуры с казахским и другими алфавитами, адаптации ПЭВМ и других внешних устройств средств ВТ к общению с ними на казахском и других языках народов, населяющих республику;

– организации передачи научно-технической информации, документов и писем на казахском языке и других национальных языках на базе республиканской информационно-вычислительной сети (РИВС) и представляемых ею информационных услуг;

– разработки и внедрения в учебных заведениях, центрах информатики ускоренных методов обучения казахскому языку с применением ЭВМ, мегафонной и аудиовизуальной техники;

– создания и внедрения на базе ПЭВМ систем, обеспечивающих машинный построчный перевод с казахского на русский язык и обратно, а также для других национальных языков.

Успешная реализация программы информатизации на основе вышесформулированных принципов во многом будет опре-

деляться от степени решенности следующих вопросов:

– информатизация не должна противопоставляться другим важнейшим народнохозяйственным программам по продовольствию, жилью, товарам народного потребления или конкурировать с ними, а быть их составной частью, обеспечивая достижения сформулированных в них целей;

– необходимо обеспечить всемирную демократизацию процессов производства и потребления информатизации, общедоступность информационных ресурсов и услуг; ликвидацию необоснованных зон закрытой информации; защиту прав личности от информационного вторжения;

– гласность и открытость формирования приоритетов информатизации, которые должны соответствовать реальным общественным потребностям;

– нецелесообразно использовать критерий экономической эффективности как единственный показатель оценки результатов информатизации. Такой сложный социальный феномен, как процесс информатизации, требует комплексной оценки его эффективности в социальной, политической, идеологической и других сферах общественной деятельности.

ОБЩАЯ МОДЕЛЬ И ПОНЯТИЯ ИНФОРМАТИЗАЦИИ РЕСПУБЛИКИ

На основе анализа существующих подходов к решению проблем информатизации в стране / 3...5, 15...21 / и зарубежом / 6...12/ с учетом приложенных принципов и цели информатизации можно построить общую модель описания процессов информатизации республики (рис. 1). В данной модели использованы следующие обозначения: ПЭВМ – персональная ЭВМ; АРМ – автоматизированное рабочее место; ЭС – экспертная система; БД – банк данных; БЗ – банк знаний; РСБД – республиканская система БД; ППП – пакет прикладных программ; ВЦКП – вычислительный центр коллективного пользования; РАСС – республиканская автоматизированная сеть связи; РСПД – республиканская система передачи данных.

Согласно общей модели информатизации республики (ОМИР)

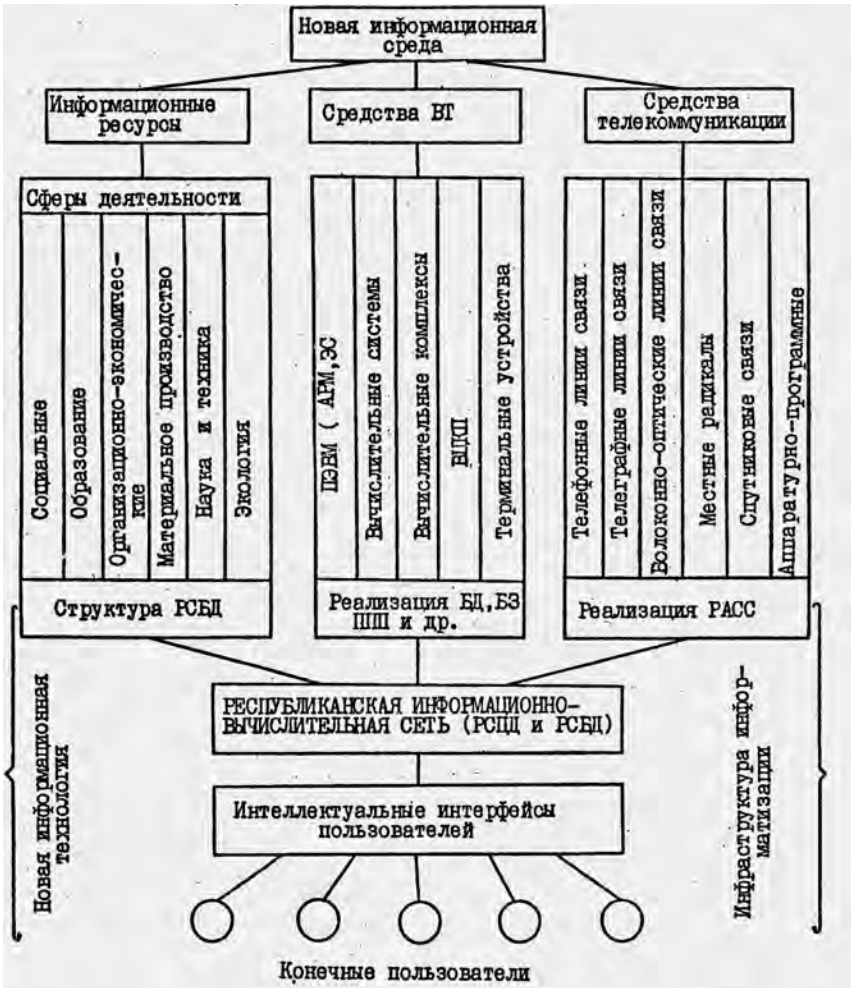


Рис. 1. Общая модель информатизации республики

можно выделить 3 основные составляющие информатизации:

1) новая информационная среда;
2) новая информатизационная технология (НИТ);
3) инфраструктура информатизации республики.

14

Новая информационная среда – совокупность информационных ресурсов, средств вычислительной техники и средств передачи данных (телекоммуникации), которые обеспечивают информационное обслуживание всех сфер деятельности общества.

Новая информационная технология – комплекс методов и средств, обеспечивающих целостную технологию сбора, передачи, обработки, хранения и представления информации с учетом основных закономерностей развития информационной среды.

Инфраструктура информатизации – совокупность территориально разнесенных средств вычислительной техники и информационных ресурсов, объединенных в единую систему посредством республиканской системы передачи данных и обеспечивающих всевозможные сетевые взаимодействия конечных пользователей в информационной среде.

Из ОМИР следует, что новая информационная среда в совокупности с методами и средствами НИТ образует инфраструктуру информатизации, технической базой которого является республиканская информационно-вычислительная сеть (РИВС). Каждый из составляющих информатизации, в свою очередь, включает в себя множество элементов. Поэтому более подробно остановимся в каждом из этих элементов и дадим их определения.

Например; новая информационная среда состоит из 3 важнейших элементов:

1) информационных ресурсов, соответствующих различным сферам деятельности общества и реализуемых в виде РСБД;

2) средств вычислительной техники, включающих в себя терминальные устройства (ТУ), ПЭВМ, вычислительные системы (ВС), вычислительные комплексы (ВК), ВЦКП, БД, БЗ, ППП, АРМ, ЭС, системы автоматизации проектирования (САПР), операционные (ОС) и сетевые системы (СС) и др.;

3) средств передачи данных (телекоммуникаций), состоящих из телеграфных, телефонных, волоконно-оптичес-

ких линий связи, местных радиоканалов, спутниковых связей и аппаратно-программных средств коммуникаций, которые в совокупности образуют РАСС.

Под информационными ресурсами будем понимать совокупность общечеловеческих (или общеобразовательных) и специальных (профессиональных) знаний, накопленных в обществе как продукт интеллектуальной деятельности человека. К общеобразовательным относятся такие знания, которые даются в детских дошкольных учреждениях, школах и средних учебных заведениях, а также общие знания о различных сферах деятельности в обществе. К специальным знаниям можно отнести научно-технические, производственно-технические, управленческие, социальные и другие виды знаний.

Таким образом, информационные ресурсы становятся непосредственным продуктом интеллектуальной деятельности наиболее квалифицированной и творчески активной части трудоспособного населения страны / 15 /. В сложившихся социально-экономических условиях перехода к рыночным отношениям сравнительная ценность информационных ресурсов по отношению ко всем остальным национальным ресурсам имеет явную тенденцию к возрастанию.

Под РИВС будем понимать комплекс территориально разнесенных ЭВМ, ВС, ВК или ВЦ, объединенных в единую сеть с помощью РСПД и обеспечивающих пользователям дистанционный доступ и коллективное использование информационных, вычислительных и сетевых ресурсов.

Распределенная система передачи данных (РСПД) представляет собой совокупность каналов связи, коммуникационных средств и аппаратур передачи данных.

Вычислительная система – совокупность физически и программно связанных процессоров, образующих параллельную систему, обеспечивающую одновременное выполнение нескольких арифметико-логических операций.

Вычислительный комплекс – ассоциация ЭВМ, физически объединенных в единую систему параллельной обработки информации под управлением общей операционной системы.

Терминальное устройство (ТУ) предназначено для орга-

низации взаимодействия пользователя с ресурсами РИВС.

Сетевая система – система, обеспечивающая взаимодействия конечных пользователей РИВС.

Автоматизированное рабочее место (АРМ) – инструментальное средство, ориентированное на автоматизацию профессиональной деятельности специалиста, реализованное на ПЭВМ.

Банк данных (БД) – хранилище интегрированных и коллективно используемых специальных баз данных, организованное таким образом, чтобы обеспечить независимость структур хранимых данных от типов устройств памяти и обрабатывающих программ, оптимизировать использование памяти и время доступа.

Банк знаний – совокупность общеобразовательных или профессиональных баз знаний о предметных и проблемных областях, организованная таким образом, чтобы обеспечить независимость языков общения и систем управления банками данных (СУБД) и знаний (СУБЗ).

Республиканская система банков данных (РСБД) – совокупность информационно совместных ведомственных, региональных и локальных банков данных и банков знаний, реализуемых на РИВС.

Экспертная система (ЭС) – инструментальная система программирования, символьного представления и обработки знаний экспертов предметной области, эвристического поиска и выдачи рекомендаций при решении задач на уровне высококвалифицированного специалиста.

Таким образом, в каждой информационной сфере образуются локальные, региональные и отраслевые БД и БЗ, которые реализуются в виде распределенной структуры РСБД. Физическая реализация БД, БЗ, АРМ, ЭС, ППП и других систем осуществляется на ПЭВМ, ВС, ВК и ВЦКП, а набор каналов связи, коммуникационных средств и АПД реализуют РСПД.

Новая информационная технология в отличие от обычной технологии обработки данных должна быть единой для любых видов информационного обслуживания и обладать следующими

характерными признаками:

– персонализация вычислений на основе массового внедрения ПЭВМ и автоматизированных рабочих мест (АРМ);

– интеллектуализация интерфейсов пользователя с информационной средой (ПЭВМ, АРМ, ЭС, БД, БЗ и др.);

– автоматическая формализация общеобразовательных и профессиональных знаний на основе создания баз данных и баз знаний;

– применение локальных и распределенных сетей передачи данных.

При этом НИТ должна состоять из следующих составляющих: новой технологии телекоммуникации на основе локальных и распределенных вычислительных сетей; новой технологии обработки информации на основе использования аппаратно-программных средств искусственного интеллекта (ИИ) и создания экспертных систем (ЭС).

В соответствии с направлениями информатизации можно выделить следующие сферы внедрения НИТ: здравоохранение, образование, материальное производство, непроизводственная сфера, экология, организационно-экономическая система, наука и техника, сеть массового обслуживания.

Конечной целью информатизации республики является создание инфраструктуры отрасли информатики, которая представляет из себя взаимосвязанный комплекс РСБД, и республиканской информационно-вычислительной сети, состоящей из совокупности СВТ и РСПД.

Теперь рассмотрим основные проблемы информатизации республики.

ПРОБЛЕМЫ СОЗДАНИЯ НОВОЙ ИНФОРМАЦИОННОЙ СРЕДЫ

Для создания новой информационной среды требуется решить 2 важнейших вопроса:

1) определить основные информационные сферы деятельности и их структуры;

2) создать и развить комплекс промышленной индустрии

(КПИ) средств вычислительной техники, телекоммуникации и информатики с привлечением силы как союзных, так и иностранных фирм.

Для решения первого вопроса в соответствии с характером использования информационных ресурсов можно производить работы по следующим основным направлениям информатизации: социальной сферы; сферы образования, подготовки и переподготовки кадров; организационно-экономического управления народным хозяйством республики; сферы научных исследований, проектирования и технологической подготовки производства, сферы материального производства; сферы охраны окружающей среды.

Успешное решение второго вопроса прежде всего зависит от формирования в структуре народного хозяйства республики межотраслевого комплекса, призванного обеспечить разработку, производство, обращение и поддержку применения средств вычислительной техники, телекоммуникации и информатики.

Основной целью решения вышеуказанных вопросов является обеспечение эффективности информационного обслуживания населения республики. Поэтому в процессе создания новой информационной среды следует учесть и решить следующие задачи:

- обеспечение эффективности, точности и достоверности преобразования знаний в информацию;
- выбор способов организации информационного взаимодействия различных групп пользователей;
- изучение и прогнозирование информационных потребностей республики;
- определение информационных структур различных сфер деятельности общественности республики;
- управление информационными ресурсами различных сфер деятельности;
- обеспечение безопасности и защиты информации;
- обеспечение удобства эксплуатации информационных ресурсов потребителями;
- совершенствование служб передачи и обработки информации;

– комплексное развитие различных направлений информатизации республики;

– разделение труда между производителями и потребителями информационных ресурсов.

Большинство из перечисленных задач должно быть решено не только путем разработки и создания новых СВТ и средств телекоммуникации, но с широким внедрением методов и средств НИТ, базирующихся на применении элементов искусственного интеллекта.

Новая информационная технология

Отчислительной особенностью новой информационной технологии является использование методов и средств систем искусственного интеллекта, т.е. интеллектуализация технических, программных и организационных средств для сбора, передачи, обработки, хранения и представления информации. Поэтому НИТ – принципиально новый тип технологии, объединяющий в себе /22/:

– новую технологию телекоммуникации на основе локальных, региональных и глобальных информационно–вычислительных сетей (ИВС);

– новую технологию обработки информации на основе ПЭВМ, АРМ, ЭС, интеллектуальных систем и др.;

– новую технологию общения и принятия решений, использующую средства искусственного интеллекта: базы знаний, языки общения с ЭВМ на естественном языке, системы логического анализа и вывода, распознавания образов и ситуаций, накоплении знаний и др.

Следует подчеркнуть, что в перспективе основу новой технологии телекоммуникации прежде всего будут составлять цифровые сети интегрального обслуживания (ЦСИО). Концепция ЦСИО (ISDN) заключается в создании сетей, в которой одни и те же средства телекоммуникации обеспечивают передачи данных, речи и изображений. При этом в таких сетях используются как способы коммутации каналов, так и коммутации пакетов, что способствует расширению диапазо-

на представляемых сетевых услуг.

Рассмотрим отличительные особенности новых технологий обработки и принятия решений от традиционной информационной технологии. На рис. 2. приведена схема традиционной технологии решения задачи на ЭВМ, где использованы следующие обозначения: БСФ – библиотека стандартных функций; ППП – пакет прикладных программ; СУБД – система управления базами данных; ПУ – печатающее устройство; ГУ – графическое устройство; ТУ – терминальное устройство.

Информатизация общества означает массовое использование СВТ во всех сферах деятельности человека. Разумеется, профессиональных программистов не хватит, чтобы обеспечить решение данной проблемы. А именно, традиционная технология решения задач на ЭВМ характеризуется наличием посредников между ЭВМ и конечными пользователями, к которым относятся аналитики (прикладные математики), программисты и операторы ЭВМ (или информационные работники) / 16 /. На рис. 2. им соответствуют уровни 2-й и 3-й. При этом конечный пользователь дает концептуальное описание задачи на своем профессиональном языке, т.е. формулируется концептуальная модель. Аналитик на основе концептуальной модели задачи пользователя разрабатывает математическую модель и алгоритм решения задачи. В результате исходная задача с языка конечного пользователя переводится на язык прикладного математика.

На 3-м уровне осуществляется разработка программы с использованием языка программирования. Далее программа и исходные данные вводятся в ЭВМ информационным работником (или оператором) с помощью ТУ (4-й уровень) и соответствующих управляющих программ системных программных средств. После этого происходит трансляция программы с языка программирования на машинный язык ЭВМ, т.е. получение рабочей программы. Для этой цели используются системные программные средства, БСФ, пакеты программ (6-й уровень). Затем осуществляются выполнение программы и выдача результатов к пользователю.

Такой подход организации информационной технологии

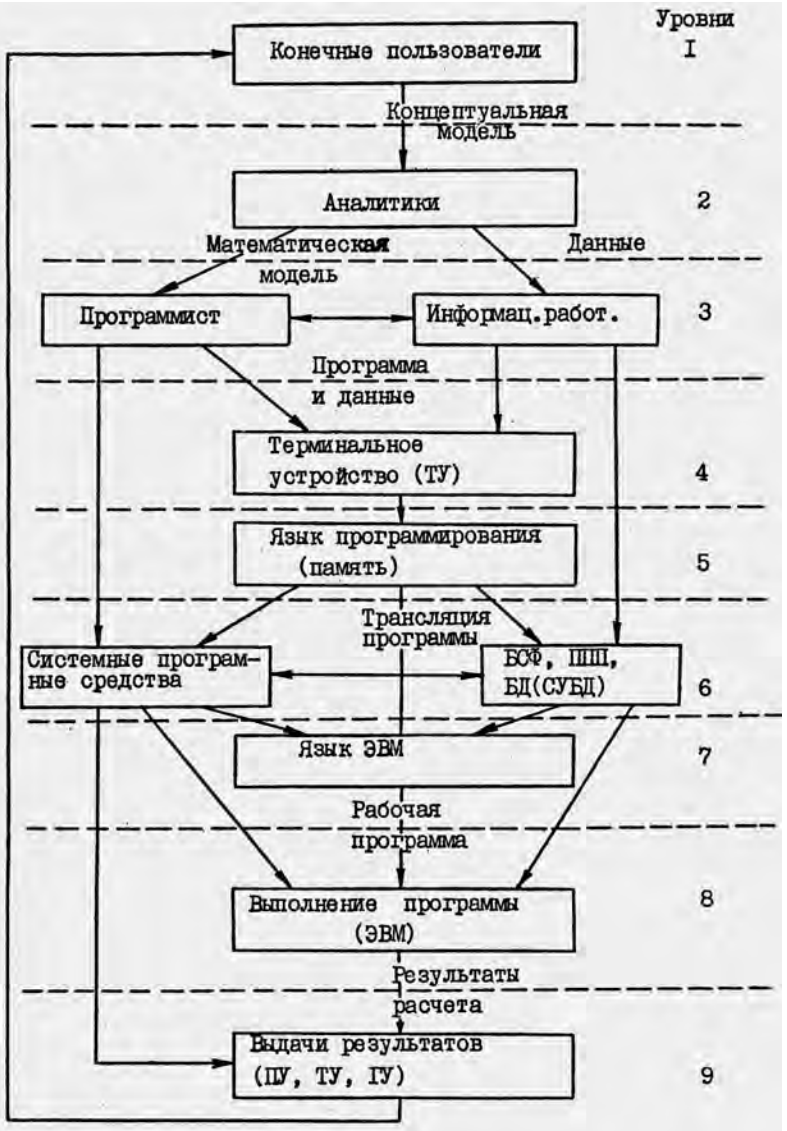


Рис. 2. Традиционная информационная технология

имеет низкую эффективность, большое время ожидания результатов, зависимость пользователя от других специалистов посредников, которые могут исказить его представление о решаемой задаче и интерпретации результатов. Поэтому в настоящее время сложные задачи на современных ЭВМ решаются в основном с использованием ППП, мощных БД. Для этой цели в традиционной технологии используются интерфейсы связи с ЭВМ, в качестве которых выступают: языки высокого уровня, языки запросов к БД, генераторы прикладных программ, генераторы отчетов и др.

Однако традиционная информационная технология не позволяет в полной мере использовать потенциальные возможности СВТ, чтобы достичь максимальной эффективности при создании различного типа и назначения системы на их базе. Это объясняется тем, что 80 % информации, используемой в настоящее время в различных областях жизни, имеет нечисловой характер (речь, печать, графика, изображения и т.д.), которые трудно поддаются к обработке на современных ЭВМ, находящихся в эксплуатации.

Для успешного решения этой проблемы в источнике / 23/ предлагается руководствоваться концепцией четырех " И ": информатизация интеллектуализация, интеграция и индивидуализация. Известно / 22 /, что последние 3 концепции лежат в основе создания НИТ и рассматриваются как их наиболее характерные признаки.

Концепция интеллектуализации предполагает, что системы, создаваемые на основе НИТ, должны обладать следующими свойствами:

– уметь вести непосредственный диалог с непрофессионалами пользователями на естественном языке, в том числе в речевой форме, или путем обмена графическими информациями, с помощью интеллектуальных интерфейсов:

– иметь механизмы создания и накопления знаний о предметных или проблемных областях;

– воспринимать и манипулировать знаниями, подвергать к ассоциативной обработке информации и делать логические выводы, т.е. решать задачи пользователей без составления

программ.

На рис. 3. приведена схема НИТ, в которой в отличие от традиционной технологии отсутствуют 2,3 и 5, соответст-

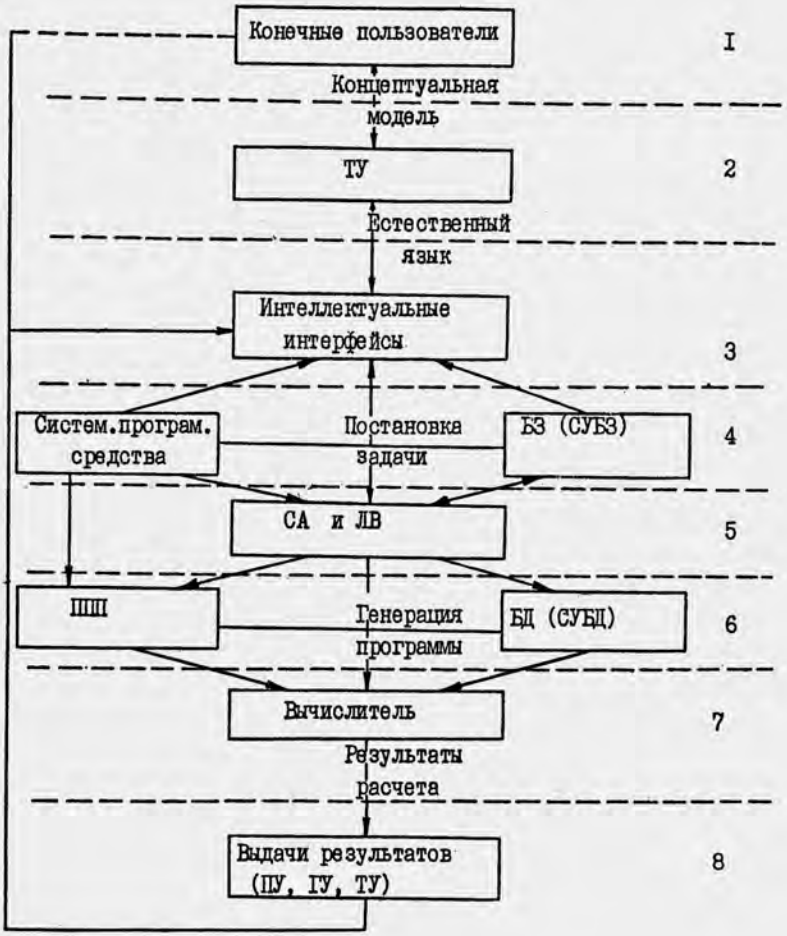


Рис. 3. Новая информационная технология

вующие аналитикам, программистам, информационным работникам и языкам алгоритмического программирования. Вместо них в НИТ появились 3–5 уровни, соответствующие интеллектуальным интерфейсам, БЗ с СУБЗ, система анализа и логического вывода (СА и ЛВ). Данные уровни обеспечивают реализацию концепции интеллектуализации информационных технологий с вышеперечисленными свойствами.

Такой подход реализации НИТ основывается на основе использования методов и идей, полученных в области искусственного интеллекта. Следовательно, успех создания НИТ будет зависеть от решения основных проблем искусственного интеллекта. К ним относятся / 26...30/:

П р о б л е м а п р е д с т а в л е н и я з н а н и й, связанная с решениями задач формализации и представления знаний в памяти интеллектуальных систем (ИС). Для этого разрабатываются специальные модели представления знаний, языки их описания и выделяются различные типы знаний. Изучаются источники, из которых ИС может черпать знания, и создаются процедуры и приемы с помощью которых возможно приобретение знаний о проблемной области для ИС.

П р о б л е м а м а н и п у л и р о в а н и я з н а н и я м и, заключающаяся в оперировании знаниями для принятия решения. В рамках данного направления строятся способы пополнения знаний на основе их неполных описаний, изучаются системы классификации хранящихся в ИС знаний, разрабатываются процедуры обобщения знаний и формирования на их основе абстрактных понятий, создаются методы достоверного и правдоподобного вывода на основе имеющихся знаний; предлагаются модели рассуждений, опирающихся на знания и имитирующих особенности человеческих рассуждений.

П р о б л е м а о б щ е н и я пользователя с ЭВМ (ИС), т.е. создания интеллектуальных интерфейсов. Данная проблема заключается в:

– понимании связных текстов на формализованном (огра-

ниченном) и неформализованном естественном языках и синтез соответствующих текстов;

– понимании информации в речевой форме и синтез речи;

– разработке теории моделей коммуникации между человеком и ИС, связанных с интеграцией в единый внутренний образ сообщений различной модальности (речевых, текстовых, зрительных и т.п.);

– формировании объяснений к действиям ИС, которые она должна уметь порождать по запросам пользователей.

На основе исследований в этом направлении формируются методы построения лингвистических процессоров, вопросно-ответных систем, диалоговых систем и других ИС, целью которых является обеспечение комфортных условий для общения человека с ИС.

П р о б л е м а в о с п р и я т и я включает в себя задачи:

– анализа трехмерных сцен;

– разработки методов представления информации о зрительных образах в БЗ;

– создания методов перехода от зрительных сцен к их текстовому описанию и методов обратного перехода;

– разработки процедур когнитивной графики;

– создания средств для порождения зрительных сцен на основе внутренних представлений в ИС.

Считается, что имеются большие возможности в повышении уровня интеллектуальности ИС за счет обработки зрительной (образной) информации и соотнесения ее с обработкой символьной (текстовой) информации.

П р о б л е м а о б у ч е н и я предполагает, что ИС способны к обучению, т.е. решению задач, с которыми они ранее не встречались. Для этого необходимо:

– создать методы формирования условий задачи по описанию проблемной ситуации или по наблюдению за этой ситуацией;

– научиться переходу от известного решения частных задач к решению общей задачи;

– создать приемы декомпозиции исходной задачи на мел-

кие так, чтобы они оказались для ИС уже известными;

– разработать нормативные и декларативные модели самого процесса обучения;

– создать теорию подражательного поведения.

Проблема организации поведения заключается в разработке специальных поведенческих процедур, которые позволили бы им адекватно воздействовать с окружающей средой, другими ИС и пользователями. Для достижения такого взаимодействия надо провести исследование в ряде направлений и создать:

– модели целесообразного поведения, нормативного поведения и ситуативного поведения;

– специальные методы многоуровневого планирования и коррекции планов в динамически изменяющихся ситуациях функционирования ИС.

Концепция интеграции основывается на том, что во всех сферах человеческой деятельности усиливаются интеграционные тенденции. Интеграция является одной из главных концептуальных идей на современном этапе развития научно-технического прогресса, в том числе проблемы информатизации. Так как сама информация представляет собой удобный способ:

– представления знаний в концентрированной форме или в виде перевода на удобный язык;

– воссоздания забытых знаний;

– формирования новых знаний путем использования процедур эвристического и логического выводов.

Кроме того, новая информационная технология также представляет собой интеграцию нескольких технологий, т.е. / 22 /:

– работы с первичными данными пользователей;

– создания и ведения БД и БЗ;

– сбора, регистрации и передачи данных;

– обработки и преобразования информации;

– машинной графики;

– взаимодействия конечных пользователей с ЭВМ.

Эти информационные технологии в свою очередь опираются

на следующие группы взаимосвязанных функциональных средств (базовых элементов) НИТ:

– получения, сбора, ввода информации (датчики, терминалы, читающие автоматы, речевой ввод и т.д.);

– хранения информации (ОЗУ, ПЗУ, БД, БЗ и т.п.);

– передачи информации (СПД, ЛВС, ЦСИО и др.);

– обработки, преобразования информации (ЭВМ, ВС, ВК, интерфейсы и др.);

– представления, использования, вывода информации (дисплеи, индикаторы, графопостроители, принтеры и т.п.).

Главное в развитии перечисленных компонентов НИТ – обеспечение полной и стандартной интеграции их в целостные технологические системы, объединяющие основные и вспомогательные процессы в технологии обработки информации / 22/. При этом интеграция может осуществляться на уровне конечных пользователей; учреждений, организаций и предприятий; ведомостей и отраслей экономики; республики.

Интеграция на уровне пользователей осуществляется путем последовательного перехода ко все более простым, удобным и эффективным интегрированным комплексам прикладных программ, а также более сложным и комплексным ПЭВМ, терминальным и другим техническим устройствам. В результате создаются АРМ, ЭС, ИС, САПР и др. на ПЭВМ. Решение задачи интеграции на остальных трех уровнях осуществляется с помощью локальных, учрежденческих, региональных и глобальных информационно-вычислительных сетей.

К о н ц е п ц и я и н д и в и д у а л и з а ц и и в НИТ сводится к учету индивидуальных особенностей пользователей при создании СВТ, систем различного назначения, например, при создании функционально ориентированных АРМ, ЭС, автоматизированных систем, рабочих станций и др. Индивидуализация проявляется также в поддержке стремления пользователей использовать потенциальные возможности СВТ для самостоятельной организации своего рабочего места.

Первым шагом в решении проблемы индивидуализации явилась организация терминального доступа пользователей к ЭВМ, которая сильно сократила число посредников между

конечными пользователями и ЭВМ (см. рис. 3). При этом создаются программные продукты, которые конечный пользователь, имеющий навык работать с клавиатурой терминала, может использовать для решения несложных задач или для получения информации. Естественно, следующим шагом в этом направлении является использование интеллектуальных интерфейсов пользователей.

Таким образом, искусственный интеллект, как основа НИТ, умножает интеллектуальные ресурсы общества, поскольку взаимодействие пользователя с ЭВМ на своем профессиональном языке интенсифицирует его интеллект, увеличивает объем его знаний и усиливает способности к логическому выводу. В конечном итоге широкое использование методов и средств искусственного интеллекта в НИТ обусловило создание индустрии интеллектуальных систем.

Успешное решение проблем информатизации во многом будет определяться состоянием создания теории и средств НИТ, которые только начинают формироваться. Решить эту проблему можно только на основе комплексных междисциплинарных исследований объективных процессов структурного и функционального развития информационной техники и технологии как нового вида социальных коммуникационных систем.

Создание инфраструктуры информатизации республики

Функциональная направленность процесса информатизации, те принципиально новые информационные технологии, которые предстоят внедрить, требуют качественно нового фундамента, который получил емкое определение инфраструктуры информатизации республики. Ее основными составляющими должны быть: республиканская информационно-вычислительная сеть (РИВС); республиканская система банков данных (РСБД), реализуемая в РИВС; комплекс промышленности информатики (КПИ).

Совокупность средств ВТ и РСПД образует республиканскую информационно-вычислительную сеть, являющуюся техни-

ческой основой инфраструктуры информатизации республики.

Данная проблема требует решения следующих задач:

– создание базовой и зональных сетей РСПД на базе цифровых сетей связи как с коммутацией каналов, так и с коммутацией пакетов;

– создание локальных сетей как низовых структур информационной инфраструктуры;

– дальнейшее развитие структуры информационных вычислительных центров коллективного пользования (ВЦКП);

– разработка и создание шлюзовых средств комплексирования ВЦКП, локальных и региональных сетей с базовой сетью и между собой;

– развитие основных служб информатизации: электронные почты, конторы и издания, видиотекс, телефакс, телеметрия, телетекс, кабельное телевидение и т.д.;

– создание республиканской информационно–вычислительной сети;

– разработка и реализация в РИВС республиканской системы банков данных, включающей в себя распределительные банки данных (РБД) и банки знаний (РБЗ);

– набор республиканских межотраслевых систем, таких, как республиканская автоматизированная система централизованного ведения классификаторов (РАСЦВК), республиканская автоматизированная система научно–технической информации (РАСНТИ), республиканская автоматизированная система ведения фонда алгоритмов и программ (РФАП) и ряд других;

– система сервисного обслуживания процесса информатизации в части внедрения и эксплуатации средств вычислительной техники и информатики путем предоставления широкого комплекса информационно–вычислительных и технических услуг.

Первоочередной задачей реализации инфраструктуры информатизации является создание телекоммуникационной среды (РСПД), включающей в себя средства связи и передачи данных, оконечные аппаратуры пользователей и технологию использования среды (рис. 4). Основу такой РСПД должна составлять базовая сеть передачи данных (БСПД), объеди-

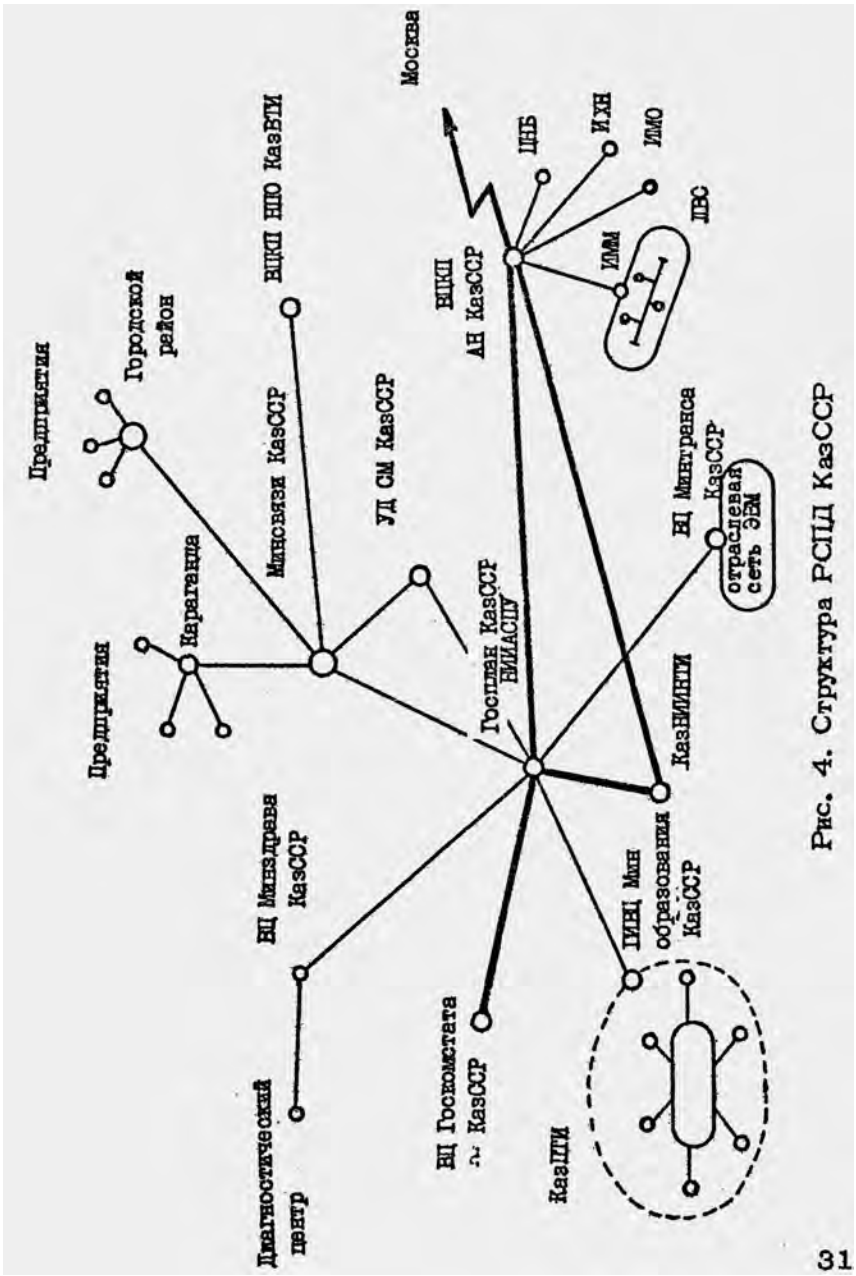


Рис. 4. Структура РСПД КазССР

31

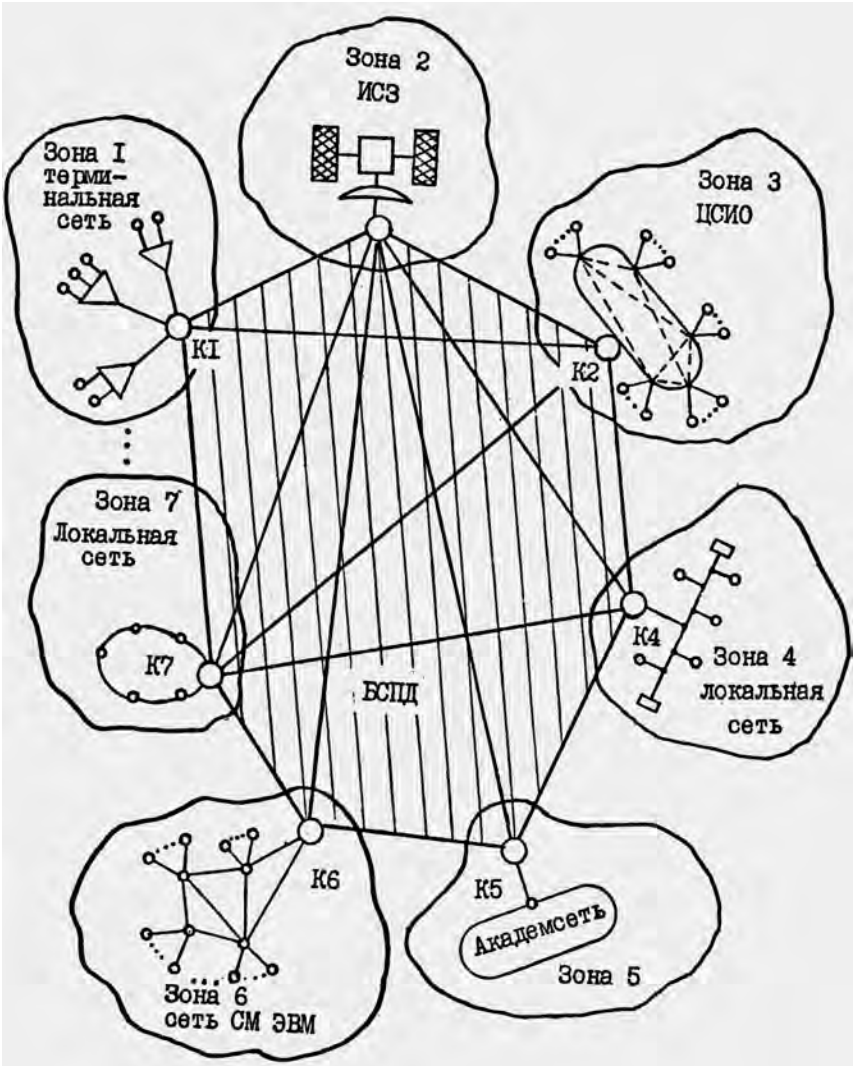


Рис.5. Структура базовой сети РСПД КазССР

32

няющая в единую систему локальные и региональные сети (рис. 5). / 31, 32 /.

РСПД Казахской ССР является открытой для дальнейшего развития системы и строится по модульному принципу, включая в себя базовую сеть передачи данных (сеть коммутации каналов, пакетов) и зональные сети передачи данных, строящиеся, возможно, на протоколах, отличающихся от протоколов базовой сети (терминальные сети СМ ЭВМ, локальные сети, ЦСИО, спутниковые сети связи с помощью искусственных спутников земли (ИСЗ) "Горизонт" и др.). Базовая сеть обеспечивает передачу информации между узлами РСПД областного значения, абоненты сети могут подключаться либо к базовой сети, либо объединяться с помощью зональных сетей с дальнейшим подключением к базовой сети (см. рис. 4).

В сложившихся условиях использования средств связи и вычислительной техники считается целесообразным строить РСПД КазССР в соответствии с государственными стандартами в области сетей и систем передачи данных, рекомендациями Международного консультативного комитета по телефонии и телеграфии (МККТТ) и международной организации стандартов (МОС или ISO). В табл. 1 показана архитектура стандартов, рекомендуемых организациями по стандартизации применительно к семиуровневой модели взаимодействия открытых систем (ВОС ISO).

Исходя из основного направления в развитии средств связи в 1991-2000 гг., предусматривающего переход на новые технические средства, освоение волоконно-оптических, лазерных и спутниковых передающих сред, планируется последовательное внедрение в РСПД КазССР цифровых сетей связи и средств коммутации информации.

Так, если в первой очереди РСПД КазССР заложены такие параметры, как передача данных между узлами базовой сети в синхронном режиме со скоростью 3400 бит/с, вероятность безотказной работы каждого тракта передачи не менее 0,96, достоверность передачи информации при использовании устройств защиты от ошибок 10^{-6}, то с переходом

Таблица 1

Уровень модели ВОС		Стандарт			
		ISO	МККТТ	ECMA	IEEE
1		2	3	4	5
7	Прикладной	8571, 9040, 9041, 8883	X.400, X.401 X.410, X.411 X.430	85	-
6	Представительный	8822, 8823, 8825, 6937, 8613	X.408, X.409, X.420	84, 86 87, 88	-
5	Сеансовый	8326, 8327	X.215, X.225	75	-
4	Транспортный	8072, 8073	X.214, X.22	72	-
3	Сетевой	8348, 8473 8208, 8648	X.25/3	92	802,1
2	Канальный	8802/2 8802/3 8802/4	X.25/2	82, 89, 90	22C 802.2 MAC 802.3,

Продолжение табл. 1

1	2	3	4	5
	8802/5			802.4, 802.5, 802.6.
1 Физический	8802/3, 8802/4 8802/5	X.21	81, 80	802.3, 802.4, 802.5, 802.6

на цифровые средства передачи и коммутации могут быть достигнуты скорости от 64 кбит/с до нескольких Гбит/с с вероятностью ошибок 10^{-8} – 10^{-5} на знак. Помимо перечисленных параметров ожидается значительное упрощение аппаратуры сопряжения терминального оборудования с каналами связи по сравнению с существующими аналоговыми коммутационными оборудованиями.

Последовательное внедрение цифровых средств передач и коммутации позволит перейти в рамках РСПД КазССР в 1996–2005 гг. к созданию цифровой сети интегрального обслуживания (ЦСИО).

Основной доступ абонентов в ЦСИО осуществляется по двум каналам передачи данных со скоростью передачи 64 кбит/с каждый и одному каналу со скоростью 16 кбит/с, что обеспечивает скорость 144 кбит/с. Интегральной частью системы ЦСИО является обеспечение скорости до 2Мбит/с при использовании 30 В-каналов и одного Д-канала для подключения АТС, имеющих

35

выход в общую сеть.

Передача информации в ЦСИО определяется протоколами X.30 и X.31, а также протоколом X.25 в режиме виртуальных каналов и коммутации пакетов.

ЦСИО обеспечивает интерактивное обслуживание 8 пользователей и обеспечивает как телесервис (реализация протоколов уровней 1-7), так и сетевые услуги (протоколы уровней 1-3).

На основе использования ЦСИО и интеллектуального интерфейса пользователя получат развитие основные сферы и службы информации республики - телефонизация, факсимальная связь, передача неречевой информации, текстовая, речевая и факсимильная почта, видеотекс, а также видеотелефон, передача изображений и файлов, электронное издательство, широковещательные теле- и радиопрограммы.

Наряду с созданием ЦСИО получат развитие средства ВТ, периферийное и терминальное оборудования, программные средства и интегрированные банки данных.

Широкомасштабное внедрение новейших СВТ и средств связи позволит создать информационную инфраструктуру, отвечающую современным требованиям к скорости, надежности, живучести и достоверности передачи информации.

Создание инфраструктуры в полном объеме является очень капиталоемким процессом, поэтому целесообразно выделить опытные зоны информатизации (районы, города, области), где проведение всех работ будет осуществляться в опережающем режиме.

Основные показатели развития РСПД и отрасли связи в целом в 1991-2005 гг. приведены в табл. 2.

Говоря о второй важной составляющей инфраструктуры информатизации РСБД, следует отметить, что она представляет собой аккумилированный информационный потенциал республики. Создание РСБД обеспечивает координацию создания важнейших БД общего назначения и проведения единой технической политики при разработке локальных баз данных на отдельных объектах отраслей экономики. Предполагается, что объем хранимой информации в РСБД будет увеличиваться при-

Таблица 2

Показатель	Значения по пятилеткам			Всего за
	1991-1995гг.	1996-2000гг.	2000-2005гг.	1991-2005гг.
1	2	3	4	5
Объем продукции отрасли – всего, млрд.руб.	3,5	5,65	8,64	17,8
в том числе РСПД, млрд.руб.	0,075	0,38	0,38	1,44
Объем услуг РСПД населению, млрд.руб.	0,0025	0,074	0,27	0,35
Капитальные вложения – всего, млрд.руб.	1,05	1,69	2,05	4,79
в том числе на РСПД, млрд.руб.	0,085	0,24	0,34	0,66
Затраты на НИОКР, млрд.руб.	0,075	0,14	0,23	0,45
Основные фонды на конец пятилетки – всего, млрд.руб.	2,25	3,59	5,4	11,24

37

Продолжение табл. 2

1	2	3	4	5
в том числе: РСПД, млрд.руб.	0,075	0,28	0,54	0,69
Численность занятых (на конец пятилетки) – всего, тыс.чел.	80	82	86	
в том числе на РСПД, тыс.чел.	2,5	7,7	10,8	
Количество основных телефонных аппаратов (на конец пятилетки), млн шт.	2,5	4,1	6,7	
Количество основных абонентских точек – всего, млн.шт.	0,1	0,51	0,55	
в том числе ЭВМ и ПЭВМ, млн шт.	0,0025	0,12	0,54	

мерно в 4...5 раз за пятилетие как путем расширения сфер информационного обслуживания, так и за счет роста информационных потребностей общества.

Для создания РСБД Казахстана необходимо решить следующие вопросы:

- изучить информационные потребности по основным направлениям информатизации и сформулировать систему заказов на создание соответствующих частей РСБД;
- определить головные министерства и ведомства, а также организации-соисполнители по направлениям информатизации и поручить им участие в создании РСБД с последующим обеспечением их функционирования;
- разработать комплекс руководящих методических, нормативно-правовых материалов и инструментальных средств, обеспечивающих создание, функционирование и развитие РСБД Казахской ССР на основе типовых проектных решений и накопленного опыта в других союзных республиках;
- обеспечить проектирование, разработку и внедрение локальных и ведомственных БД и РСБД в целом;
- сформулировать организационно-правовой статус РСБД;
- организовать регистрацию БД, создаваемых в республике, и создать автоматизированную службу их учета;
- разработать экономический механизм для процессов обмена данными и для тиражирования РБД и РБЗ.

В табл. 3 приведены оценочный состав и характеристики первоочередных банков данных РСБД.

НАПРАВЛЕНИЯ ИНФОРМАТИЗАЦИИ РЕСПУБЛИКИ

Обеспечение качественно нового уровня решения всего комплекса проблем, возникающих перед обществом в управлении, производственной, общественной и политической деятельности, в быту и организации досуга, сформированное в качестве главного требования при решении задач информатизации, обязывает обозначить ключевые направления информатизации, на которых предстоит сосредоточить внимание. При этом основополагающим должно стать стремление напра-

Таблица 3

Наименование БД	Количество информационных объектов (млн шт.)	Объем, Гбайт
1	2	3
Общественное производство		
продукция	2,3	1,3
нормативы на производство	1,8	1,3
нормативы на работы и услуги	0,023	0,69
чертежно-конструкторская и строительная документация	16,1	34,9
предприятия, организации, колхозы, кооперативы	0,01	0,04
установленное оборудование	1,3	1,3
производственные помещения	0,4	0,69
объекты капитального строительства	0,004	0,012
Транспорт		
транспортные пути и пункты	0,04	0,24
транспортные средства	1,3	1,3

Продолжение табл. 3

1	2	3
Наука и техника	0,23	1,15
Финансы и кредит	20	3,45
Социальная сфера		
жилой фонд	4,6	2,3
здравоохранение	13,8	13,8
справочная служба	-	2,3
библиотеки, каталоги, памятники искусства	11,5	2,3
Демографические данные	13,8	27,6
Объекты административно-территориального деления	0,0018	0,003
Общесоюзные классификаторы	1,38	0,28

вить максимум в информатизацию непроизводственнной сферы и первичных звеньев народного хозяйства - предприятий, объединений, организаций и учреждений. Это означает, что упраздняется сложившаяся на практике приоритетность разработки организационно-экономических АСУ и их верхних звеньев в рамках РАСУ. Информатизация снизу вверх - это стратегически новый взгляд на предстоящие разработки.

Одной из главных проблем информатизации является создание функционально-ориентированных информационных технологий для следующих сфер деятельности: здравоохранения, образования, экологии, бытового обслуживания, культуры, науки и техники, материального производства, непроизводственной сферы, организационно-экономической системы, се-

ти массового обслуживания.

Информатизация социальной сферы

В функциональной направленности информатизации приоритет отдается социальной сфере, в частности внедрению новых информационных технологий в здравоохранении, банковской системе, экологии, образовании, социальном обеспечении, культуре и общественной жизни, а также в непроизводственных отраслях (коммунально-жилищном хозяйстве, бытовом обслуживании, торговле, транспорте и др.).

Внедрение методов и средств НИТ в здравоохранении сводится к созданию и внедрению:

- автоматизированных систем (АС) профилактического, диагностического и консультационного обслуживания населения, которые могут быть стационарными, передвижными и дистанционными;
- автоматизированных систем контроля и слежения за здоровьем населения, предназначенных для проведения диспансеризации основных инфекционных и сердечно-сосудистых, опухолевых заболеваний, диабета;
- автоматизированных систем управления скорой медицинской помощью, клинико-диагностическими лабораториями, клиническими больницами;
- распределенных банков данных "здравоохранение", банков данных по эмпирической медицине и др.;
- технологии электронного медицинского паспорта и "Истории болезни";
- АС обработки и анализа медико-статистической и планово-экономической информации о ресурсах и деятельности органов и учреждений здравоохранения в условиях внедрения системы страховой медицины и рыночных отношений;
- АС планирования, учета и контроля в аптечных учреждениях;
- АРМ и ЭС для врачей-специалистов, учета и расстановки медицинских кадров;
- автоматизированных обучающих систем (АОС) подго-

товки, переподготовки и аттестации медицинских работников;

– АС учета, контроля и управления процессами снабжения, распределения, монтажа, ремонтажа и технического обслуживания медицинской техники в областных центрах республики;

– АС обработки научно-медицинской информации.

Информатизация в области медицины позволит:

– усилить профилактическую направленность здравоохранения, повысить качество медицинского обслуживания и обеспечить постепенный переход к ежегодной диспансеризации всего населения;

– оценить индивидуальное и общественное здоровье, анализировать взаимосвязь здравоохранения с другими сферами общественной жизни (в первую очередь с охраной окружающей среды и социальным обеспечением) и их влияния на сохранение и укрепление здоровья населения;

– анализировать тенденцию развития научных исследований в разных направлениях медицины, выдавать диагностические новинки и их описание, осуществлять диагностические консультации, вести разработку прогнозов здоровья населения страны, городов, сел, регионов в зависимости от действия антропогенных, геофизических, производственных, социально-психологических факторов.

В сфере банковского обслуживания населения предстоит усовершенствовать информатизацию сберегательного дела на основе комплексной автоматизации технологии банковского производства. При этом необходимо уделять первоочередное внимание созданию новых технологий платежного обслуживания населения; применению экономико-математических методов для высокоэффективного управления банковской деятельностью, внедрению современных носителей финансовой информации и необходимой номенклатуры специализированных технических средств. Осуществить поэтапное внедрение типовых проектных решений комплексной автоматизированной системы безналичных расчетов населения за товары и услуги (КАСБР).

Информатизация в области банковского обслуживания населения позволит:

– сократить оборот наличных денег на основе введения новых платежных средств в виде кредитных карточек;

– укрепить денежное обращение в республике;

– повысить качество и сократить сроки обслуживания населения по всем видам расчетно–кассовых операций торговыми, коммунальными, бытовыми и другими организациями.

Важнейшим вопросом социальной жизни человека как с точки зрения здравоохранения, так и экологии является информатизация его трудовой деятельности. Использование информационной технологии в качестве нового типа коммуникаций между членами общества должно привести к существенным изменениям содержания многих видов труда. Например, интеллектуализация основных видов профессиональной деятельности позволит максимально реализовывать творческий потенциал людей и повысить культуру труда, эти технологии существенно способствуют ликвидации тяжелого и малоквалифицированного труда. При этом изменяются условия труда, которые в минимальной степени вредны для человека. Информатизация создает и качественно новые возможности для контроля за состоянием условий и процесса труда с помощью новейших приборов контроля и управления. Все это будет способствовать сохранению здоровья человека и защиты окружающей среды.

К социальным результатам, которые можно достигнуть путем информатизации о б р а з о в а н и я относятся:

– повышение среднего уровня интеллектуальности общества за счет роста качества информации и персонализации обучения, расширения возможностей самообразования и переквалификации;

– раннее выделение способностей детей и адекватное дифференцированное их обучение;

– снижение возрастного ценза для включения в трудовую деятельность из–за сокращения средних сроков обучения.

В области о б щ е с т в е н н о й ж и з н и необходимо обеспечить членам общества более широкий доступ к различным источникам информации и к индивидуальным средствам ее обработки, включение их в мировую систему широкого не–

регламентированного распространения информации. Это позволит формировать личность с широкими интересами, стремление к духовному совершенствованию и гуманизму. Для этой цели необходимо создать автоматизированные системы проведения референдумов, опроса и учета мнения по различным вопросам жизни общества, юридической помощи и др.

В области развития к у л ь т у р ы особое внимание должно уделяться информатизации библиотечного дела, кинофикации, организации и функционированию выставок, музеев, информационно-справочному обслуживанию населения, охране архитектурно-исторических памятников.

Для успешного решения вышеперечисленных задач требуется создать комплекс АС ведения библиотечно библиографических информационных процессов, музейного дела, управления кинопрокатом, театральной, концертной и репертуарной деятельностью, обучения и повышения квалификации работников культуры, АРМ специалистов служб и управлений культуры. Внедрение новых форм досуга и отдыха населения на основе информационных технологий в центрах культуры и досуга, парках культуры и отдыха и т.д.

В жилищных вопросах целесообразно автоматизировать процессы организации и управления решением жилищной проблемы, включая разработку долгосрочной обоснованной программы, увязанной и сбалансированной с решением основных проблем развития областей, городов, районов и сел; обеспечить анализ, оценку и управление реализацией долгосрочной программы на основе формирования годовых и пятилетних планов, управление текущим распределением жилой площади; выявление, учет и использование всех жилищных ресурсов; обмен и замену жилых помещений и др.

Основные проблемы внедрения НИТ в жилищно-коммунальном хозяйстве заключаются в создании комплекса АС и АРМ жилищного и гостиничного хозяйств, организаций энергоснабжения, водоснабжения, теплоснабжения и благоустройства, ремонтно-строительных организаций, предприятий газификации и топливоснабжения.

В сфере б ы т а предстоит использовать средства информа-

тики для сокращения непроизводительных затрат на решение бытовых проблем за счет внедрения электронных систем для заказов товаров и услуг, контроля за состоянием коммунально-бытовой техники, АС распределения и учета жилищного фонда. Необходимо решить задачу формирования информационной среды жилого помещения, насыщения бытовой техники встроенными средствами информатизации, а также организации обучения пользования информационными средствами. Кроме этого, требуется разработать и внедрить в эксплуатацию типовые информационные технологии в виде АС и АРМ в специализированные предприятия и территориальные организации управления бытового обслуживания.

В сфере т о р г о в л и внедрение НИТ должно обеспечивать: рост уровня потребления населения, определяемый повышением качества и количества товаров, поступающих в торговые сети; значительное повышение уровня комфортности жизни за счет развития сферы услуг в системе торговли – автоматизация заказов товаров из дома, "электронные" магазины, безналичные расчеты и т.д.

Первоочередными задачами использования НИТ в торговле являются разработка и внедрение АС оперативно-диспетчерского управления сетями торговли и общественного питания, АРМ работников хозрасчетных предприятий торговли в розниче, опта, общественном питании, в производственных звеньях потребкооперации республики.

Внедрение НИТ в транспорте прежде всего сводится к созданию автоматизированных систем массового обслуживания:

– бронирования и продажи авиабилетов "Сирена-2" в Алма-Ате, Караганде, Чимкенте, Кустанае, Целинограде, Актюбинске;

– бронирования и продажи железнодорожных билетов "Экспресс-2" в республике.

Создание информационных структур в социальной сфере позволит повысить качественный уровень жизни трудящихся, создать более высокий психологический и культурный комфорт, уменьшить затраты рабочего времени на удовлетворе-

ние бытовых нужд. В полной мере будут реализованы такие демократические механизмы, как выборы, референдумы, опросы общественного мнения и т.п. Практически неограниченным будет объем оказываемых бытовых услуг (коммерческие, транспортные, информационно-справочные и др.).

ИНФОРМАТИЗАЦИЯ ОБРАЗОВАНИЯ, ПОДГОТОВКИ И ПЕРЕПОДГОТОВКИ КАДРОВ

Для успешного развития процессов информатизации исключительно важны проблемы образования и подготовки кадров. Учитывая неотложность решения этих вопросов, при дефиците вычислительных ресурсов, следует использовать самые различные формы приобщения к информационным технологиям на основе компьютерных технологий обучения, включающих диалоговые автоматизированные обучающие системы, тренажеры, экспертнообучающие системы с базами знаний и т.д. Для этого необходимо:

– в соответствии с концепцией непрерывности образования решить вопросы организации "сквозной" компьютеризации образования по цепочке "школа-ПТУ-вуз-профессиональная деятельность". Для этой цели необходимо создать специализированные классы на основе дешевых ПЭВМ (в вузах – АРМов), объединенных в локальные сети и автоматизированные обучающие системы. Широко развернуть кружковую работу с компьютерами во Дворцах пионеров, включая районные и дворовые компьютерные клубы, развернуть шефскую работу предприятий и организаций, имеющих СВТ. Поддерживать создание коммерческих компьютерных центров обучения и досуга;

– открыть кафедры или специализации по информатике во всех вузах республики. Особое внимание обратить на создание соответствующих кафедр в педагогических вузах;

– в технических вузах, в соответствии с их специализацией, предусмотреть создание локальных вычислительных сетей с распределенными базами данных и целевыми АРМ (конструктора, технолога, агронома, бухгалтера, эконо-

миста). Внедрить обязательное выполнение курсового и дипломного проектирования на вычислительных комплексах, а также выполнение студентами платных производственных заказов;

– в аспирантуре и докторантуре обеспечить подготовку высококвалифицированных научных и научно–педагогических кадров в соответствии с приоритетными направлениями по информатике и ВТ;

– широко использовать кооперативные и совместные предприятия (учебные центры) по подготовке кадров. Практиковать расширение обучения стажировки студентов и молодых специалистов в ведущих вузах страны и за рубежом;

– разработать трансляторы и другие средства общения с ЭВМ на казахском и русском языках. С накоплением опыта, по мере необходимости, создавать трансляторы на языках других национальных групп населения республики (уйгурский, корейский, немецкий и т.д.). Необходимо использовать средства информатики для взаимного перевода с одного языка на другой.

Результатом практической реализации вышеперечисленного комплекса мер должно быть решение следующих вопросов:

– создания отраслевого и региональных центров новых информационных технологий образования (НИТО) в системе народного образования, которые должны стать ведущими организациями в области разработки и внедрения методов и средств НИТ в образовании;

– разработки научно–методических основ информатизации образования;

– разработки и реализации инфраструктуры информатизации образования в составе РИВС как совокупности взаимосвязанных ЛВС школ, техникумов, вузов и региональных ИВС областей;

– создания локальных, региональных и отраслевых систем БЗ и БД;

– разработки типовых программных средств НИТО для автоматизированных систем обучения (АОС), АРМ и ЭС;

– разработки методов и средств НИТО на казахском язы-

ке;

– разработки и внедрения комплектов программируемых электронных игрушек, компьютерных тренажеров, обучающих систем и игр в детские дошкольные учреждения;

– создании типовых АОС, экспертных обучающихся систем (ЭОС), АРМ и педагогических программных средств для системы школьного образования, в том числе школ с обучением на казахском языке;

– создании специализированных АОС, ЭОС и АРМ по профилям подготовки и переподготовки кадров в вузах, техникумах и ПТУ, в том числе – на казахском языке.

Динамика изменения контингента учащихся в республике и потребность в средствах вычислительной техники соответственно приведены в табл. 4 и 5.

Таким образом, предлагаемый комплекс мер и решение проблем информатизации образования должны:

– создать необходимые условия завтрашнего решения острейших проблем социально-экономического и научно-технического преобразования в стране;

– помогать многим миллионам школьников и студентов, облегчить условия работы сотням тысяч педагогов школ, техникумов и вузов;

– дать толчек пересмотру устаревших педагогических концепций и развитию всей системы непрерывного образования;

– повысить уррвень компьютерной грамотности населения и информационной культуры;

– обеспечить доступность знаний и данных для каждого члена общества;

– развить интеллектуальные и творческие способности индивидума (с учетом его самостоятельности, самобытности и т.п.);

– повысить квалификацию или изменить сферу профессиональной деятельности в течение жизни каждого члена общества;

– обеспечить гуманитаризацию общего образования и воспитания, всеобщее компьютерное обучение, эффективное заочное и "домашнее" образование;

Таблица 4

Количество учащихся, тыс.чел.

Учебные заведения	1986–1990 гг.	1991–1995 гг.	1996–2000 гг.	2001–2005 гг.
Школы	3522,5	3610	3730	3850
Вузы	273,4	291	310	340
ПТУ	282,13	313	351	385

Таблица 5

Потребность в АРМ (тыс. шт.) и средствах ВТ (млн руб.) для сферы народного образования

Учебные заведения	1986–1990 гг.		1991–1995 гг.		1996–2000 гг.		2001–2005 гг.	
	АРМ	ВТ	АРМ	ВТ	АРМ	ВТ	АРМ	ВТ
Школы	0,88	8,8	3,67	36,7	11,75	117,5	20,5	205
Вузы	0,273	2,73	0,873	8,73	1,55	15,5	1,7	17
ПТУ	0,211	2,1	0,51	5,1	1,24	12,4	1,61	16,2

– интенсифицировать учебный процесс и повысить качество образования путем индивидуализации процессов обучения.

Информатизация сферы научных исследований, проектирования и технологической подготовки производства (НИР, ПКР и ТПП)

При высоких требованиях к качеству выпускаемой продукции, темпам ее обновления, росту ее номенклатуры, сокращению сроков разработки, созданию и освоению новых процессов и технологий, изделий и материалов, а также к качеству проектов значительно возрастают объемы работ в сфере научно–исследовательских (НИР), проектно–конструкторских работ (ПКР) и технологической подготовки производства (ТПП). Так, по машиностроительному комплексу, с учетом динамики показателей по объему производства товарной продукции; индексу изменения и обновления основной номенклатуры; доле продукции и коэффициенту роста технико–экономических характеристик продукции, выпускаемой на мировом уровне объем работ по НИР, ПКР и ТПП возрастает в 6 раз.

Цель информатизации НИР, ПКР и ТПП состоит в ускорении получения и углубления научных знаний о явлениях и закономерностях в природе, технике и обществе; в сокращении сроков проведения разработок и повышении качества на этапах жизненного цикла продукции и технологий " Исследование–проектирование и конструирование–подготовка производства".

Для этого в области приобретения, накопления и использования информационного ресурса необходимо создание комплекса автоматизированных рабочих мест и систем, обеспечивающих поиск и анализ первоисточников, автоматизацию исследовательских, экспериментальных и проектно–конструкторских работ (АРМ, САПР, АСНИ и др.), документирование, расширение сферы профессионального общения. Приобретенным направлением информатизации НИР, ПКР и ТПП является создание банков данных и банков знаний, докумен–

тальной и фактографической информации.

Это позволит:

– изменить стиль и поднять уровень в области НИР, ПКР и ТПП, ускорить получение новых знаний, проектно-конструкторских решений, исключить дублирование и повысить их качество;

– получить оперативный доступ к информационным ресурсам, накопленным в республике, стране и за рубежом, устранить запаздывание в получении информации;

– своевременно информировать о новых результатах потенциальных потребителей.

Оценка масштабов информатизации НИР, ПКР и ТПП, при принятом росте производительности (результативности) автоматизированного рабочего места (АРМ) за 1991–2005 гг. в 5 раз, показывает, что доля занятых автоматизированным трудом в сфере НИР, ПКР и ТПП к 2005 г. достигнет 50 %; удельный вес объема работ, выполняемых с применением вычислительной техники, повысится до 89 %; уровень фондовооруженности специалистов средствами микропроцессорной и вычислительной техники поднимается до 11 тыс. руб. на человека и будет выполнен возросший объем работ по НИР, ПКР и ТПП. Потребность сферы НИР, ПКР и ТПП в средствах микропроцессорной и вычислительной техники приведена в табл. 6.

Информатизация организационно-экономического управления

Управление на уровне республики с ее многоотраслевой экономикой в условиях интенсификации народного хозяйства, совершенствования методов управления и экономического механизма, демократизации общества, расширения гласности и самостоятельности предприятий не может обойтись при выборе альтернативных и согласованных решений без автоматизации процессов принятия решений на основе использования интегрального информационного ресурса республики. При этом математическое моделирование, вычислительный эксперимент,

Таблица 6

Потребность в АРМ (тыс. шт.) и ВТ (млн руб.)
для сферы НИР, ПКР и ТПП

Отрасаль промышленности	1986-1990 гг.		1991-1995 гг.		1996-2000 гг.		2001-2005 гг.	
	АРМ	ВТ	АРМ	ВТ	АРМ	ВТ	АРМ	ВТ
1	2	3	4	5	6	7	8	9
Вся промышленность	3,36	68	13,3	525,4	18,8	1162,2	13,01	968,4
В том числе:								
машиностроение и металлообработка	1,04	20,8	4,8	192	8	480	4	400
черная металлургия	0,17	3,48	0,78	30,27	0,76	42,3	0,66	36,6
цветная металлургия	0,28	5,69	0,91	35,6	1,13	66,7	0,75	76,0
топливная промышленность	0,3	6,8	1,32	51,8	1,82	107,8	1,44	104,7

Окончание табл. 6

1	2	3	4	5	6	7	8	9
электроэнергетика	0,15	3,16	0,65	25,5	0,91	53,8	0,82	42,86
химическая и нефтехимическая промышленность	0,21	4,11	0,84	33,14	1,34	79,5	0,97	78,12
лесная и деревообрабатывающая промышленность	0,07	1,5	0,26	10,19	0,37	20,5	0,29	20
промышленность промстроймате-риалов	0,18	3,64	0,65	25,6	0,84	50	0,75	45,6
легкая промышленность	0,45	9,02	1,5	58,6	1,8	106,5	1,63	84,34
пищевая промышленность	0,51	10,2	1,5	62,8	1,8	109,1	1,7	80,2

системный анализ, прогноз, генерация и оценка вариантов, методы оптимального планирования должны быть составной частью системы информационного обслуживания и выступать в качестве математической поддержки процессов познания и принятия решений на всех уровнях управления. С этой целью необходимо развить информационные инфраструктуры межотраслевых, отраслевых и территориальных народнохозяйственных комплексов в области планирования и управления на всех уровнях системы хозяйствования республики.

В первую очередь необходимо создать информационную инфраструктуру на уровне Совета Министров Казахской ССР – Автоматизарованную систему обработки информации для директивных органов (АСОИДО); на уровнях республиканских межведомственных функциональных органов; Единую автоматизированную технологию планирования Госэкономкомитета Казахской ССР (ЕАТП); Единую статистическую информационную систему Госкомстата Казахской ССР (ЕСИС); Автоматизированную систему финансовых расчетов Минфина Казахской ССР (АСФР); Автоматизированную систему Госкомтруда Казахской ССР–АСУ "Труд и социальное развитие; Автоматизированную систему управления материально–техническим снабжением республики–АСУ МТС; автоматизированные системы банковских операций Государственного и других банков в республике; 16 отраслевых автоматизированных систем управления. На уровнях территориальных народнохозяйственных комплексов: АСУ народным хозяйством Северо–Казахстанской области; АСУ городским хозяйством Алма–Аты.

Информатизация сферы управления на уровне предприятий республики связана с задачей создания информационных инфраструктур промышленных предприятий и объединений, обеспечивающих качественно новое решение всего комплекса задач, выдвигаемых производством, и направленных на повышение производительности труда, качества выпускаемой продукции, а также культуры производства. Для этого необходимо создать программно–аппаратные средства, обеспечивающие построение многоуровневых производственно–вычислительных сетей, объединяющих локальные сети цехов, участков и функ-

циональных служб, систем сбора и обработки первичных данных о работе оборудования и выполнении производственных заданий, анализ экологической обстановки и решение других функций жизнедеятельности предприятия. Последовательная интеграция и интеллектуализация автоматизированных систем обработки данных и управления в сфере производства – одно из приоритетных направлений информатизации общества, обеспечивающее высокие темпы научно-технического прогресса, динамизм его развития.

Коренная перестройка управления экономикой, необходимость обеспечения ускорения научно-технического прогресса и социально-экономического развития республики приведут у значительной потребности в повышении качества принимаемых управленческих решений на всех уровнях.

Важное место при этом занимает создание автоматизированных рабочих мест различного управленческого назначения, информационно-вычислительных сетей, системы телекоммуникаций, распределенных баз данных и баз знаний предприятий и организаций, вычислительных центров коллективного пользования и других средств, позволяющих:

– обеспечить общественный контроль за соотношением меры труда и меры потребления различных категорий и социальных групп населения, социально-справедливо распределять материальные и духовные блага общества благодаря всеобщему и универсальному учету во всех сферах деятельности и в результате широкого доступа общественности к этой информации;

– разрабатывать научно обоснованные и сбалансированные комплексные планы социально-экономического развития республики, отраслей, регионов и предприятий и следить за их выполнением.

Расчет масштабов информатизации сферы управления, при принятом росте производительности (результативности) автоматизированного места (АРМ) за 1991-2005 гг. в 2 раза, показывает, что доля занятых автоматизированным трудом в сфере управления к 2005 г. достигнет 48 %; удельный вес объема работ, выполняемых с применением вычисли-

тельной техники поднимается до 8,1 %, уровень фондовооруженности специалистов средствами вычислительной техники повысится до 5,7 тыс. руб. на человека.

Потребность сферы материально-экономического управления средствами микропроцессорной и вычислительной техники приведены в табл. 7.

Таблица 7

Потребность в АРМ (тыс.шт.) и СВТ (млн руб.) для сферы управления

Численность работников сферы управления – 146 тыс. чел.	1986–1990 гг.	1991–1995 гг.	1996–2000 гг.	2001–2005 гг.
АРМ	1,89	12,55	10,22	8,76
ВТ	18,9	251,12	306,6	525,6

Информатизация сферы материального производства

В основе информатизации сферы материального производства должны лежать 2 основных концептуальных положения: интеграция и технологический прорыв в производстве.

Интеграция в этом направлении информатизации должна поддерживать и развивать общие интеграционные тенденции в производственной сфере и обществе в целом, гибко сочетаясь с концепцией индивидуализации и специализации.

Технологический прорыв через информатизацию сферы материального производства заключается в органическом сочетании информационных технологий с производственными, обеспечивая новое качество производственной сферы – интеллектуальные работы, манипуляторы, гибкие

производственные системы и модули, заводы-автоматы и т.д.

Информатизация производственных систем

Информатизация производственных систем будет происходить в двух направлениях: информатизации технологических агрегатов и технологических процессов на базе встраиваемых микропроцессорных средств; информатизации управления производством.

Использование встраиваемых в технологическое оборудование микропроцессоров придаст ему новое качество, новые потребительские свойства, снизит эксплуатационные затраты. Интеллектуализация оборудования позволит оптимизировать технологические процессы, реализовывать принципы самодиагности и самопрограммирования выхода из нештатных ситуаций, создать интеллектуальные интерфейс оператора с системой машин. Информатизационное оборудование будет приближаться по свойствам к роботам. В сфере материального производства помимо роботов-манипуляторов будут применяться роботы с профессиональной ориентацией, автономные интеллектуальные роботы для использования в опасных и аварийных ситуациях.

Необходимые масштабы информатизации технологического оборудования процессов и производств на базе использования средств микропроцессорной и вычислительной техники определяются с учетом достижения заданных показателей по росту объема производства, повышению фондоотдачи, производительности труда и качества продукции.

Расчет масштабов информатизации материального производства основан на выделении в структуре основных производственных фондов (их активной части) автоматизированного оборудования, оснащенного средствами микропроцессорной и вычислительной техники. При расчете приняты следующие показатели социально-экономического развития республики: объем промышленного производства за 1991-1995 гг. возрастет в 2,1 раза, в том числе по комплексу машиностроения - в 4 раза; фондоотдача за эти годы по промышленности повысится

Таблица 8

Потребность в средствах микропроцессорной (МПТ) и вычислительной техники (ВТ), измерения и контроля (ИК) для сферы производства, млрд руб.

Отрасль промышленности	1990–1995 гг.			1996–2000 гг.			2001–2005 гг.		
	ВТ	МПТ	ИК	ВТ	МПТ	ИК	ВТ	МПТ	ИК
1	2	3	4	5	6	7	8	9	10
Вся промышленность	0,728	0,285	0,145	1,509	0,563	0,373	3,02	0,844	0,830
В том числе машиностроение и металлообработка	0,15	0,06	0,03	0,41	0,15	0,105	1,01	0,28	0,28
черная металлургия	0,05	0,01	0,009	0,098	0,035	0,025	0,148	0,0042	0,042
цветная металлургия	0,072	0,032	0,016	0,151	0,055	0,038	0,193	0,064	0,052

Продолжение табл. 8

1	2	3	4	5	6	7	8	9	10
топливная промышленность	0,083	0,039	0,017	0,163	0,061	0,040	0,205	1,075	0,056
электроэнергетика	0,040	0,016	0,008	0,093	0,040	0,023	0,214	0,859	0,061
химическая и нефтехимическая промышленность	0,958	0,018	0,011	0,102	0,043	0,027	0,263	0,051	0,066
лесная и деревообрабатывающая	0,013	0,005	0,002	0,035	0,012	0,009	0,077	0,021	0,021
промышленность промстрой-									

60

Окончание табл. 8

1	2	3	4	5	6	7	8	9	10
материалов	0,040	0,016	0,008	0,085	0,031	0,012	0,202	0,056	0,056
легкая промышленность	0,125	0,050	0,025	0,0186	0,068	0,047	0,360	0,100	0,100
пищевая промышленность	0,098	0,039	0,019	0,186	0,068	0,047	0,348	0,096	0,096

на 28 %, в том числе по машиностроительному комплексу – на 50 %.

Потребность сферы производства в средствах микропроцессорной и вычислительной техники приведена в табл. 8.

Информатизация агропромышленного комплекса

Решение продовольственной программы предполагает обеспечение населения высококачественными и в достаточном ассортименте пищевыми продуктами в значительной степени на основе индустриализации и электронизации всего агропромышленного комплекса страны, включающего сельское хозяйство и перерабатывающую промышленность. Задачей информатизации агропромышленного комплекса является создание соответствующей информационной инфраструктуры сельского хозяйства и перерабатывающей промышленности на основе новых информационных технологий.

Создание информационной инфраструктуры агропромышленного комплекса позволит автоматизировать этапы сбора, обработки, хранения и передачи информации; создать для всех уровней управления и регионов комплексы технических средств с использованием ПЭВМ, локальных вычислительных систем, производственно-диспетчерских вычислительных центров коллективного пользования, диспетчерско-вычислительных пунктов в колхозах, совхозах, животноводческих комплексах, птицефермах; создать автоматизированные рабочие места бригадиров, мастеров, техников, технологов, аппарата всех звеньев управления, объединенных в локальные вычислительные сети для обмена информацией между смежными рабочими местами: специалисты агропромышленного комплекса должны иметь и использовать моноиндикаторные устройства (влагомеры и др.), групповые полевые контроль-управляющие центры, агрометеорологические станции, автоматизированные молочно-товарные фермы, автоматизированные птицефермы и свинофермы, боротовые контрольно-измерительные системы на машинно-тракторных агрегатах, боротовые управляющие системы, воздействующие на механизированный тех-

нологический комплекс; стационарные пункты с дистанционным управляющим механизированным комплексом, с автоматизированными системами по анализу состояния почвы, растений, агроклиматических условий, определению потребностей в питательных веществах; автоматизированные системы управления заводами и предприятиями по приему и обработке молока, производству масла и сыров, управлению режимами температуры, по взвешиванию и сортировке птицы на линиях, управлению линиями убоя и холодильными складами, по управлению технологическими линиями изготовления колбасных изделий, управлению линиями выпечки.

Это позволит:

– вызвать глубокие социальные изменения в сельском хозяйстве;

– моделировать мелкие и крупные сельскохозяйственные операции; оценивать генетические характеристики пород скота и культур, моделировать физические и химические изменения почвы в результате ее обработки и применения пестицидов и удобрений и др.;

– объединить весь жизненный цикл создания конечных продуктов в производстве, оперативно принимать качественные решения в управлении, максимально расширить и повысить качество услуг населению в быту и на работе;

– осуществить реальный переход на экономические методы управления.

Оценочная потребность в средствах микропроцессорной и вычислительной техники для информатизации сферы агропромышленного комплекса приведена в табл. 9.

Таблица 9

Потребность в СВТ и МПТ для сферы производства АПК, млрд руб.

Показатель	1990–1995 гг.	1996–2000 гг.	2001–2005 гг.
СВТ	0,398	0,688	1,147
МПТ	0,156	0,256	0,320
ИК	0,079	0,170	0,315

Информатизация охраны окружающей среды

В стране отсутствует единая система охраны окружающей среды, необходимость которой исключительно важна. Реализация информационных инфраструктур в этой области позволит в этой области контролировать сложные экологические процессы, планировать и осуществлять защитные мероприятия, вырабатывать предложения по развитию производительных сил и структурным изменениям в народнохозяйственном комплексе.

Для этого необходимо развернуть работы по созданию общесоюзного и региональных систем мониторингов, включающих: средства получения экспресс-информации о состоянии и динамике водных объектов, воздушной среды и почвы; систем моделирования метеорологических процессов, крупномасштабных процессов влияния научно-технического прогресса на окружающую среду; экспертных систем диагностики и прогнозирования процессов загрязнения-очистки или разрушения-восстановления экологической среды; единый экологический паспорт регионов. Необходимо использовать и передвижные станции для проведения биомониторинга окружающей среды, включающие автоматические и автоматизированные технологии анализа данных о состоянии почвы, воды и атмосферы; интеллектуальные датчики характеристик природных процессов;

системы связи с передачи данных; наводные и подводные, наземные и космические станции; проблемно-ориентированные базы данных и базы знаний; динамические модели взаимодействующих составляющих частей данного региона; программные системы для эколого-экономического моделирования и др.

В качестве приоритетного направления следует определить создание республиканской системы контроля окружающей среды (РСКП) на основе интеграции различных сетей массовых наблюдений; метеорологических, метеорадиолокационных, гелеогеофизических (ионосферных наблюдений, контроля земного магнетизма и др.), сейсмологических и пр. Следует предусмотреть взаимодействие с международными сетями и базами данных природоохранного и ресурсного характера, такими, как Международная справочная система источников информации по окружающей среде (ИНФОТЕРА); Международная информационная система по сельскохозяйственным наукам и технике (АГРИС); Глобальная система мониторинга окружающей среды (ГСМОС); Международный регистр потенциально-токсических химических веществ (МРПТХВ) и др.

Вышеперечисленный комплекс мер и их практическая реализация должны проводиться в рамках и тесной связи с республиканскими целевыми комплексными научно-техническими программами на 1991-1995 гг. и на период до 2000 г. по следующим направлениям: "Арал-2000" и "Охрана окружающей среды и рациональное использование природных ресурсов республики".

Это позволит:

- обеспечить оздоровление окружающей среды, жизни человека, животного и растительного мира;
- моделировать экологические опасные ситуации, натурные исследования которых принципиально невозможны из-за катастрофических последствий; планировать мероприятия по восстановлению экологически грязных регионов;
- осуществлять экологическую экспертизу крупномасштабных проектов, программ и планов социально-экономического развития регионов Казахстана.

ПУТИ ДОСТИЖЕНИЯ ИНФОРМАТИЗАЦИИ РЕСПУБЛИКИ

К основным элементам реализации процессов информатизации республики можно отнести:

- подготовку общества к информатизации;
- создание научных и промышленных основ информатизации республики;
- разработку организационно-экономических механизмов;
- разработку комплекса законодательных и правовых актов;
- выбор структуры организационного управления процессами информатизации на всех уровнях.

Учитывая стратегический характер информатизации в решении проблем социально-экономического развития республики необходимо сделать кардинальные и революционные шаги в области создания экономического и правового механизмов, обеспечивающих реализацию процесса информатизации. Именно информатика, в первую очередь, должна стать опытным полигоном для обработки решений, которые можно с учетом накапливаемого опыта распространять "вширь" на другие отрасли народного хозяйства.

Подготовка общества к информатизации

Непрерывная подготовка общества к информатизации требует системности, а также принятия ряда мер в области пропаганды, рекламы, подготовки и переподготовки кадров. Среди них необходимо отметить следующие:

- создать широкую сеть региональных центров информатики. В этих целях предстоит уделить внимание созданию широкой государственной и кооперативной систем от крупных и средних центров информатики в системе ГКВТИ СССР и других ведомств до мелких кооперативных. Развивать компьютерные клубы молодежи, компьютерные игротеки, игровые автоматы и аудиовизуальные средства, практиковать внесение изменений в проекты строительства жилых и других зданий и массивов с учетом выделения площадей на первых этажах под клубы,

игротеки, центры информатики. В системе народного образования создать государственные центры новых информационных технологий, организовывать на их базе разработку, внедрение и сопровождение информационных технологий образования по интегрированным учебным планам и программам, решение задач интенсификации и индивидуализации обучения и учебно-методическую поддержку центров непрерывного обучения;

– организовать в республиканской и местной печати, на радио и телевидении дискуссии по развитию информатики, уделять больше места пропаганде идей информатизации, передового опыта;

– открыть специальные курсы для руководителей и специалистов народного хозяйства с упором не столько на обучение работе на компьютере, сколько на демонстрацию возможностей информатики; организовать и практиковать изучение передового опыта;

– организовывать выпуск (ввоз) и широкую продажу населению бытовых ПЭВМ отечественного и зарубежного производства по невысоким ценам.

Развитие фундаментальных и прикладных исследований в области информатики

Успешное решение проблем информатизации республики во многом определяется уровнем развития фундаментальных и прикладных научных исследований в области информатики, вычислительной техники и систем связи, осуществляемых на базе существующих и вновь создаваемых научных учреждений в составе АН КазССР и Минобразования Казахской ССР, а также широкой кооперации с соответствующими организациями союзных республик.

В рамках координации проводимых работ, централизованного планирования и финансирования информатизации в республике предпочтение следует отдавать следующим фундаментальным и прикладным исследованиям:

– создание и освоение перспективных технологий микроэлек-

троники и инструментальной базы для изготовления сверхбольших интегральных схем (СБИС);

– разработка и развитие научных основ методик проектирования информационных технологий, базирующихся на применении соответствующих компонентов систем искусственного интеллекта (СИИ), создания БД и БЗ, САПР различных назначений, АСУ ТП, АСНИ и др.;

– разработка методов математического моделирования и вычислительных экспериментов при создании экспертных систем в прогнозировании, планировании и управлении народным хозяйством;

– создание теоретических основ и инструментальных средств комплексного проектирования РСПД, РИВС, РСБД и других составляющих инфраструктур информатики;

– проектирование научных исследований по разработке ПЭВМ, персональных вычислительных систем (ПВС), АРМ, ЭС и создание на их базе ЛВС различного назначения с возможностями общения с ними на казахском и других языках народов, населяющих республику;

– разработка шлюзовых средств комплексирования вычислительных сетей различного назначения.

В настоящее время теоретические основы НИТ в СССР созданы и требуется дальнейшее интенсивное развитие и практическое применение. Ключевыми проблемами НИТ являются создание новых технологий телекоммуникаций, обработки, общения и принятия решений с помощью ЭВМ путем использования средств информационной инфраструктуры.

В области развития средств связи и телекоммуникации серьезнейшие изменения претерпевают технологии, оборудование и виды услуг.

К основным задачам республики в развитии технологических средств связи следует отнести:

– миниатюризацию элементов сетей связи (аппаратуры коммутации, приема–передачи и др.);

– применение волоконно–оптических линий связи (ВОЛС) при создании республиканской автоматизированной связи (РАСС);

– повышение эффективности использования физической пропускной способности каналов связи и совершенствование управления связью;

– развитие РАСС на основе архитектуры открытых сетей, ЦСИО и интеллектуализации служб сетей, повышение надежности и экономической эффективности сетей связи.

Новые технологии обработки информации (данных) и принятия решений с помощью средств ВТ опираются на современные технологии программирования, требующие обеспечения промышленного производства системных базовых и прикладных программных средств (ПС). Основные проблемы создания технологии производства ПС информатизации республики состоят в следующем:

– разработка и использование языков общения с ЭВМ на ограниченном естественном языке (ЕЯ), представления знаний и описания ПС различного назначения;

– разработка методов унификации и стандартизации языковых средств;

– развитие методов и средств сборочного и конкретизирующего программирования;

– создание инструментальных средств автоматизированной разработки ПС с интеллектуальными интерфейсами (ввод в ЭВМ речи, данных, текстов, графиков, изображений и др.);

– разработка методов и средств обеспечения надежности ПС (включая тестирование, верификацию и др.);

– разработка новых технологий программирований, создание паспортов и банков технологий.

Учитывая приоритетность информатизации среди задач научно-технического прогресса, необходимо решить следующие вопросы:

– укрепить материальную базу научно-исследовательских институтов АН Казахской ССР, вузов и других организаций, ведущих разработки в области информатики современными средствами ВТ, лабораторным и метрологическим оборудованием;

– создать в структуре АН Казахской ССР и Минобразования Казахской ССР специализированные научно-исследова-

тельские институты и вуз для целенаправленного ведения исследовательских разработок, подготовки и переподготовки научных и инженерных кадров в области информатики и ВТ;

– открыть филиал центрального научно–исследовательского института связи (ЦНИИС);

– практиковать создание научно–методологических, инженерных центров и временных научных коллективов для решения крупных проблем информатизации республики на конкурсной основе. Осуществлять преимущественно финансирование программ и проектов, а не организаций и учреждений;

– развернуть работу по участию республики в Государственных научно–технических программах, а также международных научно–исследовательских программах и зарубежных научных центрах в области информатики и вычислительной техники.

Создание комплекса промышленности информатики

Казахстан, обладая всеми необходимыми сырьевыми материалами и научными разработками для производства современных элементов средств информатики, не имеет собственного производства средств ВТ и телекоммуникации. Это помимо вышеуказанных проблем не позволяет эффективно и самостоятельно развивать наукоемкие производства и технологии – основу коммерческого прорыва в современном мире и ускорении экономического развития. Республика практически не участвует в общественном разделении труда в области информатики и ВТ.

Учитывая, что важными принципами успеха процесса информатизации в республике является включение Казахстана в союзное и международное разделение труда, можно определить следующие основные направления работ:

– создать предприятия по выпуску технических средств информатики и производству программных изделий;

– закупить за рубежом основные комплектующие компоненты современных персональных ЭВМ и организовать "отверточную" сборку на государственных или совместных предприя-

тиях;

– принять кардинальные меры по формированию в структуре народного хозяйства республики комплекса промышленности информатики (КПИ).

Комплекс промышленности информатики – это межотраслевой комплекс народного хозяйтсва республики, призванный обеспечить разработку, производство, обращение (хранение, транспорт, сбыт), эксплуатацию и поддержку применения средств информатики, информационных технологий, автоматизированных систем и инструментальных средств.

Создание комплекса промышленности информатики (КПИ) в республике должно занять длительное время. Организационное оформление КПИ потребует крупномасштабных экономических, правовых и политических решений, затрагивающих зачастую взаимопротиворечивые интересы практически всех отраслей народного хозяйства. При этом необходимо определить основные тенденции развития промышленности информатики и систему организационно–экономических условий, в которых это развитие будет происходить, а также учесть эти тенденции при формировании комплекса.

Приоритетными направлениями развития КПИ являются:

– организация производства высококачественной элементной базы с опережающими показателями надежности путем создания республиканской промышленности микроэлектроники;

– сбалансированное создание и опережающее развитие инструментальных средств проектирования, изготовления и сопровождения всех средств информатики (АСНИ, САПР, экспертных систем и др.) с минимальными эксплуатационными затратами;

– строительство предприятий по производству массовых средств информатики (ПЭВМ, ПВС, АРМ ЭС, сетевые станции, интеллектуальные интерфейсы, цифровую технику связи и др.);

– высокоэффективное использование средств информатизации.

– создание систем комплексной автоматизации производства, начиная с электронизации оборудования на всех уровнях: НИИ – предприятие (объединение) – цех – участок –

71

робот – станок – изделие – контроль.

Управление процессом информатизации республики

Комплекс организационных мер управления процессом информатизации должен решить следующие вопросы:

– определить информационные потребности по основным направлениям информатизации с учетом концепции социально-экономического развития республики до 2005 г., произвести оценки затрат на информатизацию республики и ее социальные и экономические последствия в обществе;

– наметить этапы реализации республиканской политики в области информатизации, определяющей содержание и способы воздействия на звенья народного хозяйства, которые участвуют в этом процессе;

– создать оргструктуру управления развитием комплекса промышленности информатики;

– повысить эффективность управления процессами применения информационных технологий во всех уровнях и звеньях народного хозяйства и других сферах деятельности общества.

Для решения вышеперечисленных вопросов следует:

– на предплановой стадии (при разработке КПНТП, Концепции социально-экономического развития Казахской ССР, Схемы развития и размещения производительных сил и союзных документов социально-экономического развития) предусмотреть специальный раздел по развитию народнохозяйственного комплекса информатизации;

– провести в соответствии с принятым содержанием Концепции информатизации изменение организационных структур управления, имея в виду создание на хозрасчетных началах самостоятельной республиканской ассоциации "Казахинформ", и консорциума по созданию РСПД, выступающих в качестве методического и координационного органа в республике, других новых форм совместной деятельности, как составных элементов формирующегося Комплекса промышленности информатики;

– в новом составе Верховного Совета Казахской ССР об-

разовать специальную комиссию (подкомиссию) по информатизации, которая должна определять республиканскую политику, формировать законодательные акты в области информатики;

– государственную структуру управления дополнить также общественно–кооперативными сообществами. В этих целях оказать содействие в организации ряда ассоциаций в сфере информатики на добровольной основе, например: – ассоциации пользователей средств информатизации в целях повышения эффективности применения СВТ, их защиты от некачественных и дорогостоящих проектов, оказания консультационных, информационных, посреднических услуг, противодействия монополизму и правовой защите; региональных ассоциаций содействия информатизации республики, например, при местных Советах, ЛКСМ Казахстана и органах печати, в целых широкой пропаганды идей информатизации, формирования новых информационных потребностей и т.д.;

– в целях более полного анализа обеспечения координации и контроля за ходом процесса информатизации пересмотреть систему плановых показателей и увязать их с системой статотчетности.

Организационно–правовые мероприятия по ускорению информатизации должны быть нацелены прежде всего на поощрение микродеятельности, раскрепощение условий работы в производственной, проектной, пусконаладочной, посреднической, информационно–издательской и рекламной деятельности в сфере информатики, на многообразие форм и видов деятельности.

Целесообразно предусмотреть ликвидацию тарифных ставок, сдерживающих коллективные и личные интересы, зависимость окладов всецело от объемов работ, нацеливающих на затратные методы работы. Уравнять налогообложение кооперативов, госпредприятий и возможность доступа к материально–техническим ресурсам.

Разрешить создание совместных предприятий между госорганизациями, а также различные формы объединения, независимо от ведомственной принадлежности и форм собственности, упростить процедуру их создания. В целях недопущения неоправдано высоких заработков в условиях договорных

цен, имеющейся монополии вести поиск новых и гибких форм налогообложения для кооперативов и организаций, провести необходимые мероприятия по ликвидации монополии в отдельных сферах информатики.

Актуальной является задача подготовки и внесения в соответствующие органы предложений по пересмотру системы ГОСТов на АСУ, САПР, АСНИ, разработанных Госстандартом СССР, нацеливающих на производство бумажного, а не программного продукта.

Необходимо ввести положение о республиканском госзаказе в области научных и проектных работ, предусмотрев конкурсность и состязательность, осуществить на деле финансирование тем, а не организаций на контрактной (договорной) основе.

Также необходимо разработать республиканское Положение о временных трудовых коллективах (ВТК), предусмотрев их широкое использование для выполнения госзаказов и придания ВТК всех необходимых социальных гарантий.

Следует значительно расширить права регионов республики в части создания предприятий и организаций информатики, финансирования необходимых разработок, создания и распоряжения фондами в сфере информатики. Для введения ряда законодательных актов добиваться права их введения в республике в порядке эксперимента.

К другим правовым положениям информатизации общего характера можно отнести:

– охрану интеллектуальной собственности в информатике, что стимулирует творчество в данной сфере и формирует рыночные отношения для соответствующих продуктов;

– решение правовых вопросов, связанных с компьютерными преступлениями, приводящими к несанкционированным доступам к хранящейся в ЭВМ информации;

– регулирование статуса информации, что предполагает: доступную любому гражданину страны информацию, сокрытие которой недопустимо; коммерческую информацию, которая может быть объектом купли-продажи на условиях, выдвинутых ее владельцем; частную информацию о граж-

данах страны или организациях, затрагивающих их интересы, совесть, мораль и т.д., распространение которой возможно лишь при согласии на это соответствующих лиц; информацию, по тем или иным соображениям представляющую тайну; ее распространение возможно лишь с разрешения органов, уполномоченных контролировать вопросы, связанные с такой информацией.

Необходимо правовое регулирование не только определения, но и изменения статуса информации.

Участие в союзном и международном разделении труда

Участие в союзном и международном разделении труда, которое можно считать одним из реальных факторов сокращения критического отставания республики в области информатизации, должно базироваться на следующих положениях:

– процесс информатизации в республике требует активного участия Казахстана в союзном разделении труда. В свою очередь это определяет необходимость создания научного центра в Академии наук Казахской ССР и строительство предприятий по производству средств вычислительной техники, связи и программных изделий, образующих научно-технический потенциал информатизации республики;

– для обеспечения участия республики в международном разделении труда прежде всего необходимы самые решительные шаги по организации в Казахской ССР специальных экономических зон.

Накопленный мировой опыт в этой области показывает их высокую эффективность, превращение в локомотивы национальных экономик. Характерно, что к созданию специальных экономических зон прибегают не только развивающиеся страны, но и передовые капиталистические – США, Япония и др. Так, в США в 1985 г. действовало 123 зоны свободной торговли, причем во всех штатах особый упор делается на создание предприятий микро- и радиоэлектроники.

Создание специальных экономических зон небходимо организовать прежде всего на экономически неосвоенных ранее ме-

стах, на вблизи к источникам первичного и вторичного сырья, прежде всего отходов цветной и фосфорной промышленности.

Для привлечения иностранного капитала и технологии следует пойти на льготный налоговый режим, освобождение совместных предприятий от установленного налога (на 10... 15 лет), предоставить гарантии возврата вложенного капитала и права свободно переводить инвестиции и прибыль, ограничить действие КЗОТ Казахской ССР и профсоюзную деятельность в зависимости от технологичности производства.

Необходимо приложить все усилия для создания в республике совместных предприятий, работающих в сфере информатизации. Это позволит насытить рынок техникой, программными средствами и информационными услугами.

На первом этапе необходимо сосредоточиться на организации сборочных производств для решения задач насыщения народного хозяйства компьютерами, приобретения опыта и подготовки кадров. По мере развития переходить к созданию полуавтоматизированных и автоматизированных производств.

Одним из главных факторов экономического прорыва стран западной Европы, Японии, КНР и др. в разное время послужило массовое обучение студентов и молодых ученых, конструкторов и технологов за рубежом. Необходимо использовать этот опыт и организовать обучение студентов и молодых специалистов в передовых странах, подготовить новую волну специалистов, владеющих передовыми знаниями и технологиями.

ЭТАПЫ РАЗВИТИЯ ИНФОРМАТИЗАЦИИ РЕСПУБЛИКИ

Формирование этапов развития информатизации республики является важным фактором ее последовательной реализации. Их выполнение должно найти отражение в конкретных программах на соответствующие периоды.

П е р в ы й э т а п 1 9 8 9–1 9 9 5 гг. должен обеспечить:

– создание основных социальных, экономических, организационно-правовых, научных и технических условий информатизации республики;

– уточнение структуры существующей системы подготовки и переподготовки кадров в области информатики и ВТ, создание специализированного учебного заведения и развитие существующей сети вузов в соответствии с требованиями и внедрением новой информационной технологии обучения;

– развитие фундаментальных и прикладных исследований по информатике, ВТ, кибернетике, экономике, праву и другим смежным наукам на базе существующих и вновь создаваемых научных учреждений и вузов;

– реализацию процессов компьютеризации – оснащение народного хозяйства, социальной сферы, управленческой, научно-исследовательской и образовательной деятельности средствами вычислительной техники, периферийного оборудования, создание элементной и ремонтной базы;

– создание локальных вычислительных сетей с распределенными банками данных предприятий, организаций, использование существующих заделов в разработке отраслевых и территориальных сетей и автоматизированных систем;

– разработку типовых проектных решений (особенно в социальной сфере) создания сервисных систем массового обслуживания населения с подготовкой соответствующих кадров;

– проведение мероприятий по организации комплекса промышленности информатики при активном участии в союзном и международном разделении труда;

– создание опытной зоны инфраструктуры информатизации республики, структура которой приведена на рис. 6, а соответствующая структура сети связи на рис. 7, где жирными линиями выделена первая очередь РСПД.

В опытной зоне будут отрабатываться системы массового обслуживания, обеспечивающие предоставление информационных услуг для населения: автоматизированная продажа билетов на все виды транспорта; внедрение магнитных карточек (в перспективе электронных карточек) для безналичных расчетов населения; профилактико-диагностические системы медицинского обслуживания; информационно-справочная служба торговли; научно-информационное обслуживание; пусконаладка

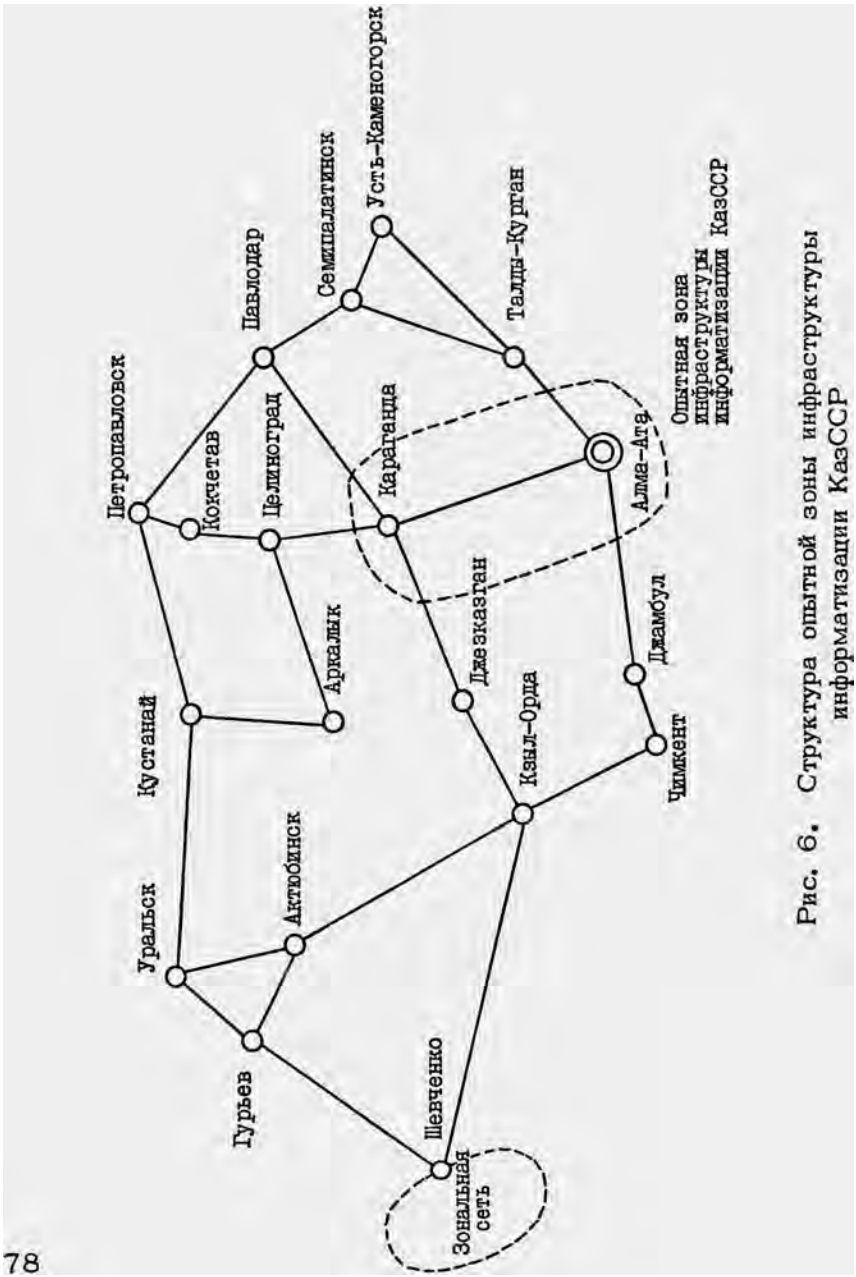


Рис. 6. Структура опытной зоны инфраструктуры информатизации КазССР

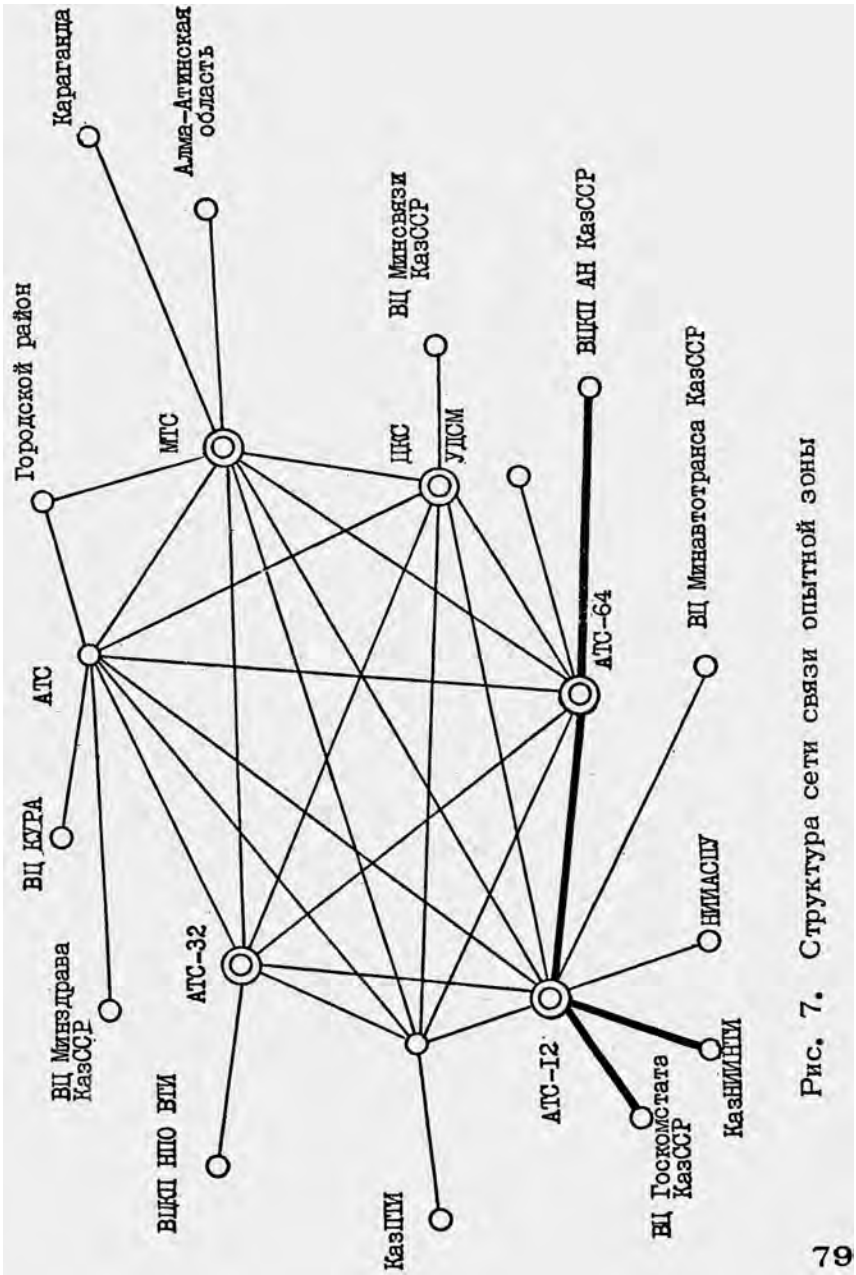


Рис. 7. Структура сети связи опытной зоны

79

техническое обслуживание средств ВТ; представление вычислительных услуг и организация досуга с использованием ЭВМ.

Второй этап 1996-2000 гг. должен обеспечить:

– углубление и расширение процесса компьютеризации и информатизации республики по всем направлениям;

– создание и освоение основных мощностей производства дешевых ПЭВМ, ПВС, АРМ, микропроцессоров и других средств ВТ и телекоммуникаций. Тем самым уровень обеспеченности предприятий, организаций и населения средствами ВТ довести до 85...95 %;

– развитие и разработка НИТ, сети коммерческих и некоммерческих банков данных и банков знаний;

– формирование республиканского комплекса промышленности информатики;

– расширение и осуществление взаимодействия опытной зоны инфраструктуры информатизации республики с союзными вычислительными сетями;

– достижение 100 % компьютеризации процесса обучения в сфере образования, подготовки и переподготовки специалистов народного хозяйства.

Третий этап 2001-2005 гг. должен обеспечить:

– создание республиканского комплекса информатизации основных сфер деятельности общества;

– завершение внедрения во все сферы жизнедеятельности человека средств информатизации: НИТ, БД, БЗ, систем искусственного интеллекта;

– массовое внедрение новейших систем массового обслуживания населения – электронная почта, электронная библиотека, электронная публикация, телетекст, видеотекс и др.;

– осуществление массовой автоматизации рабочих мест, электронизации оборудования, роботизация производства и др.;

– сокращение до минимума отставания от развитых республик и стран в области информатики с учетом перспектив развития в них процессов информатизации; создание конкурен-

тоспособного научно-технического потенциала республики.

КОНТРОЛЬНЫЕ ЦИФРЫ РАЗВИТИЯ ИНФОРМАТИЗАЦИИ И ОЦЕНКА ЕЕ ЭФФЕКТИВНОСТИ

Процесс информатизации республики в рамках данной концепции предполагает получение следующих экономических и социальных результатов:

- намечаемое увеличение объема информационно-вычислительных услуг на 1000 руб.валовой продукции отраслей народного хозяйства с 0,3 руб. в 1986 г. до 30 руб. в 2000 г. и до 45 руб. в 2005 г. позволит республике дополнительно произвести национального дохода в 14-й пятилетке 2 млрд руб. , в 15-й пятилетке - 2,8 млрд руб. за счет экономии трудовых затрат;

- повышение качества и оперативности хозяйственных решений, улучшение организационно-экономического управления можно оценить не менее чем в 4...4,5 млрд руб., достигаемое за счет экономики трудовых, материальных и финансовых ресурсов, ускорения оборота средств и предметов труда;

- внедрение АРМов конструкторов, технологов, систем автоматизированного проектирования позволяет поднять производительность их труда в 10...20 раз. В масштабах республики это можно оценить прибавкой в национальном доходе в размере 250...300 млн руб;

- внедрение систем массового обслуживания населения позволит значительно сократить непроизводительные потери рабочего времени, увеличить часть свободного времени человека на повышение культурного и образовательного уровня, снизить социальную напряженность в распределении продуктов и услуг, снизить масштабы теневой экономики в сфере услуг.

Главный результат информатизации сферы услуг и быта состоит в повышении качества и уровня жизни народа, увеличении свободного времени работающих.

Таким образом, общая контрольная сумма ожидаемого эффекта составляет 8...10 млрд руб. за 13-15-ю пятилетки.

Намеченная в концепции объемная программа информатиза-

ции требует привлечения для ее реализации существенных ресурсов. При этом в соответствии с принципом множественности источников финансирования государственный бюджет должен взять на себя от 25 % в 13-й пятилетке до 20 % в 15-й пятилетке от общего объема затрат. Остальные средства должны быть обеспечены за счет привлечения возможностей предприятий и организаций.

По заключениям экспертов, минимальная оценка затрат на информатизацию может быть представлена следующим образом:

- бюджетное финансирование НИР: 13-я пятилетка - 100 млн руб., 14-я - 100, 15-я - 100 млн руб.;
- финансирование НИР, проектных и опытно-конструкторских работ (включая программирование) за счет предприятий и областных бюджетов: 13-я пятилетка - 300 млн руб., 14-я - 400, 15-я - 400 млн руб.;
- республиканские централизованные капитальные вложения на средства ВТ и системы связи: 13-я пятилетка - 300 млн руб., 14-я - 300, 15-я - 300 млн руб.
- капитальные вложения предприятий и средства из областных бюджетов: 13-я пятилетка - 300 млн руб., 14-я - 400, 15-я - 500 млн руб.

Всего затраты на информатизацию составляют: 13-я пятилетка - 1000 млн руб., 14-я - 1200, 15-я - 1300 млн руб.

Итого за 3 пятилетки затраты составят 3,5 млрд руб., в том числе за счет бюджетных ассигнований - 1,2 млрд руб.

ЗАКЛЮЧЕНИЕ

Аналитический обзор является расширенным вариантом концепции информатизации, отражающей взгляды рабочей группы на перспективы этого процесса в республике с учетом общегосударственной стратегии СССР.

Обзор охватывает лишь основные принципиальные положения, узловые проблемы и задачи информатизации республики на концептуальном уровне с конкретным выделением приори-

тетных направлений информатизации и указанием пути их реализации. Основной целью было выявить контуры столь глобального процесса как информатизация республики, дать отправные импульсы для выработки стратегических решений по этому вопросу.

Осуществление изложенной стратегии информатизации республики возможно исключительно в условиях происходящих преобразований советского общества, улучшения политической обстановки в мире, углубления процесса демократизации и гласности, всемерного расширения самостоятельности союзных республик в решении социально-экономических задач.

Сегодня, когда мир уже вступил в эпоху так называемых информационных обществ, нельзя не отметить, что уровень развития любой страны будет определяться уровнем создания и промышленной эксплуатации национальных информационных ресурсов во всех отраслях экономики и общественно значимых сферах человеческой деятельности. Несвоевременная оценка темпов развития и решающей роли информации в обществе привело к серьезному отставанию страны от передовых стран в области информатизации. Республика же отстает от союзного уровня еще на добрый десяток лет.

Поэтому для успешного решения проблем информатизации республики требуются крупномасштабные экономические, правовые и политические решения, затрагивающие по существу взаимопротиворечащие интересы практически всех отраслей народного хозяйства, так как теперь однозначно можно утверждать, что следующим этапом развития будет формирование информационного общества.

Авторы выражают надежду, что многие читатели, ознакомившись с аналитическим обзором, смогли получить не только представление о цели и задачах информатизации, но и поняли стратегическую значимость этой проблемы в повышении интеллектуального, культурного потенциала, жизненного уровня, благосостояния всего населения республики и начнут активно участвовать в процессе информатизации.

ЛИТЕРАТУРА

1. Концепция информатизации Казахской ССР / Утверж. решением Президиума СМ КазССР от 4.09.1990 г. № 21-УШ. - Алма-Ата, 1990. - 34 с.

2. Программа информатизации Казахской ССР в 1991-1995 гг. и на период до 2005 года (проект). - Алма-Ата, 1990. - 122с.

3. Концепция информатизации советского общества (Проект) / Под ред. акад. Д.М.Гвишиани. - М.: ВНИИСИ, 1988. - 55с.

4. Концепция информатизации общества (Проект) / Под ред. акад. В.С.Михалевича. - Киев-Москва: ИК УкрАН ССР, 1988. - 56с.

5. Концепция информатизации общества / Под ред. В.Г.Захарова. - М.: ВНИИПВТИ, 1988. - 58с.

6. K l a u s H.G., M a r c h a n d D.A. Informationsmanagment in USA // Nachr.Dok. - 1989. - V.38, N4. - p.215-221.

7. W a t t e n b e r g U. Informationsmanagement in Japan // Nachr.Dok. - 1987. - V.38, N4. - p. 229-237.

8. W i n k e l A. Information resources management in Danish industrial companies / / Latul. Quart. - 1987. - V.1, N4. - p.263-270.

9. Provenzano D. European databanks on the march // Online. - 1987. - V.11, n5. - p. 17-40.

10. Sobezak K. Administracja pantwowa-informacja - informatyka (kilka problemow prawnych i organizacyjnych) // Pr.nauk. USL. Katonicach. Pr.Wydztechn. - 1986. N23. - p.68-81.

11. Rowecki S., Waszkiewicz J. Podejscie metologiczne de prognozowania rozmojn informatiki // Pr. naukorn. i prognost. - 1984. - V.3, N44. - p.41-59.

12. Boyce B.R., Kraft D.H. Principles and theories in information Science // Annu. Rew. Inf.

Sci.Techn. – 1985. – N20. – p.153–178.

13. Предложения по совершенствованию структуры промышленного производства Казахской ССР в 13-й и 14-й пятилетках: Отчет о НИР – Алма-Ата: НИЭИПиН Госплана КазССР, 1988.

14. Методика оценки масштабов информатизации на долгосрочный период: Отчет о НИР – Алма-Ата: НИИАСПУ Госплана КазССР, 1989.

15. Громов Г.Р. Национальные информационные ресурсы: проблемы промышленной эксплуатации. – М.: Наука, 1985. – 240 с.

16. Поспелов Г.С. Искусственный интеллект – основа новой информационной технологии. – М.: Наука, 1988. – 280с.

17. Глушков В.М. Основы безбумажной информатики. – М.: Наука, 1982. – 552с.

18. Свириденко С.С. Современные информационные технологии – М.: Радио и связь, 1989. – 30 4 с.

19. Семенюк Э.П. Информатика: достижения, перспективы, возможности. – М.: Наука, 1988. – 173с.

20. Информатика и компьютерная грамотность/Ответ. ред. Б.Н.Наумов. – М.: Наука, 1988. – 273с.

21. Система и средства информатики / Ответ.ред. Б.Н.Наумов. – М.: Наука, 1989. – 258с.

22. Гриценко В.И., Паньшин Б.Н. Новая информационная технология в организационных системах // УСиМ – 1988. № 1. – С.20–27.

23. Михайлевич В.С. Информатизация – важнейший ресурс перестройки советского общества // УСиМ – 1989. – № 2 – С.3–6.

24. Скурихин В.И. О формировании концепций. Концепция "четырех И" // УСиМ. – 1989. – № 2. – С.7–23.

25. Кухтенко А.И. Научный потенциал и проблема информатизации // УСиМ. – 1989. – № 2. – С.23–32.

26. Попов Э.В. Общение с ЭВМ на естественном языке. – М.: Наука, 1982. – 360с.

27. Поспелов Д.А. Ситуационное управление: Теория и практика. – М.: Наука, 1986. – 284с.

28. Искусственный интеллект: Кн. 1. Системы общения и экспертные системы: Справочник / Под ред. Э.В.Попова. – М.: Радио и связь, 1990. – 464с.

29. Искусственный интеллект. Кн. 2. Модели и методы: Справочник / Под ред. Д.А.Поспелова. – М.: Радио и связь, 1990. – 304с.

30. Искусственный интеллект. Кн.3. Программные и аппаратные средства: Справочник / Под ред. В.Н.Захарова, В.Ф.Хорошевского. – М.: Радио и связь, 1990. – 368с.

31. Сарыпбеков Ж.С., Бейсембаева М.К. Синтез структуры РВС с учетом размещения распределенных баз данных // 15 Всес.шк.–семинар по вычислительным сетям. – М.: 1990. – 119–124с.

32. Ахметов И.К., Сарыпбеков Ж.С. и др. Принципы построения и архитектура РСПД Казахской ССР // 13 Всес. шк–семинар по вычислительным сетям. – М., 1988. – С.96–101.

ОГЛАВЛЕНИЕ

Вильжан Мавлютинович Амербаев,
Абдыгаппар Ашимович Ашимов,
Жаксыбек Сарыпбекович Сарыпбеков

ИНФОРМАТИЗАЦИЯ РЕСПУБЛИКИ: КОНЦЕПЦИИ И ПРОБЛЕМЫ

Отв.редактор М.М.Макарова Редактор Н.Я.Кениг
Техн.редактор Л.А.Никитина

Сдано в набор 1.08.91. Подписано в печать 2.09.91.
Формат 60x84/16. Бум.тип. № 2.
Печать офсетная. Усл.печ.л. 5,11. Усл.кр.-отт. 25,55.
Уч.-изд.л. 3,5. Тираж 1100. Заказ 735. Цена 92 к.

Редакционно-издательский отдел КазНИИНКИ
Типография КазНИИНКИ
Адрес редакции и типографии: 480120, г.Алма-Ата,
Кирова, 221.

Опечатки

Страница	Напечатано	Следует читать
С.23 7-я строка снизу	географическими	графическими
С.31	Рис.4. Структура РСПД КазССР	Рис.6. Структура опытной зоны инфраструктуры информатизации КазССР
С.32	Рис.5. Структура базовой сети РСПД КазССР	Рис.4. Структура РСПД КазССР
С.78	Рис.6. Структура опытной зоны инфраструктуры информатизации КазССР	Рис.5. Структура базовой сети РСПД КазССР

— • —

10. Амербаев В. М., Малашевич Б. М. (авторы-составители). Сб. трудов «50 лет модулярной арифметике. Юбилейная Международная научно-техническая конференция». — М.: МИЭТ, 2005. 774 с.

ВВЕДЕНИЕ

В 2005 году исполняется 50 лет модулярной арифметике на основе системы счисления остаточных классов.

За истекшие 50 лет модулярная арифметика пережила периоды и бурного развития, и серьёзных спадов. Ведущую роль в этом направлении сыграла группа зеленоградских специалистов, возглавляемая крупными учёными в области вычислительной техники профессорами И. Я. Акушским, Д. И. Юдицким и В. М. Амербаевым. В настоящее время наблюдается

прогрессирующий рост интереса к модулярной арифметике среди разработчиков сложных систем, связанных с обработкой сигналов и изображений, с криптографией и т. п.

50-летний юбилей — хороший повод для подведения итогов и оценки перспектив модулярной арифметики. В связи с этим группа предприятий России, Казахстана, Белоруссии, США и Украины приняла совместное решение о проведении специальной юбилейной Международной научной конференцией «50 лет модулярной арифметике».

Конференция проводится в два этапа:

- заочная интернет-конференция (март — сентябрь 2005 г.),
- завершающая очная конференция в Зеленограде (МИЭТ) (сентябрь — 23–25 ноября 2005 г.).

Учитывая намечающийся синтез двух перспективных научных направлений развития вычислительной техники — модулярной арифметики и троичной системы, оргкомитет пригласил для участия в конференции учёных, разрабатывающих теории применения троичной арифметики и троичной диалектической логики при построении средств вычислительной техники.

В сборнике трудов конференции статьи участников размещены в следующем порядке: история модулярной арифметики, общие вопросы, научные разработки, прикладные разработки.

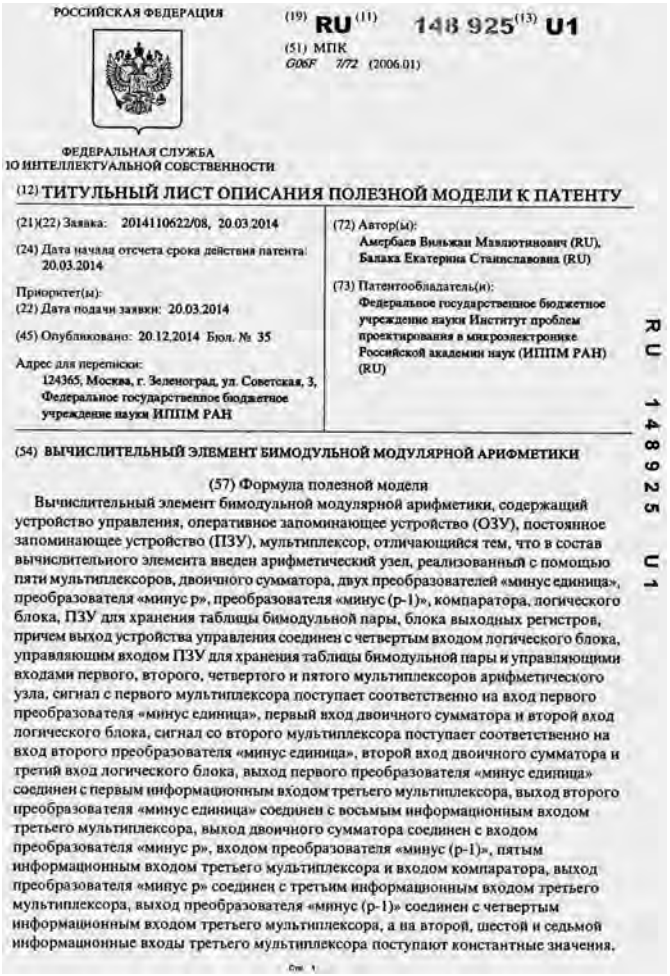
ОГЛАВЛЕНИЕ

Избранные публикации В. М. Амербаева

В настоящем разделе приведены избранные публикации В. М. Амербаева из различных сфер его научной деятельности.

Статьи расположены в хронологическом порядке.

Две последние в разделе статьи были подготовлены при жизни Вильжана Мавлютиновича, но здесь публикуются впервые.



РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **148 925** (13) **U1**

(51) МПК
G06F 7/72 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) **ТИТУЛЬНЫЙ ЛИСТ ОПИСАНИЯ ПОЛЕЗНОЙ МОДЕЛИ К ПАТЕНТУ**

(21)(22) Заявка: 2014110622/08, 20.03.2014

(24) Дата начала отсчета срока действия патента:
20.03.2014

Приоритет(ы):
(22) Дата подачи заявки: 20.03.2014

(45) Опубликовано: 20.12.2014 Бюл. № 35

Адрес для переписки:
124365, Москва, г. Зеленоград, ул. Советская, 3, Федеральное государственное бюджетное учреждение науки ИППМ РАН

(72) Автор(ы):
Амербаев Вильжан Мавлютинович (RU),
Балака Екатерина Станиславовна (RU)

(73) Патентообладатель(и):
Федеральное государственное бюджетное учреждение науки Институт проблем проектирования в микроэлектронике Российской академии наук (ИППМ РАН) (RU)

RU 148925 U1

(54) **ВЫЧИСЛИТЕЛЬНЫЙ ЭЛЕМЕНТ БИМОДУЛЬНОЙ МОДУЛЯРНОЙ АРИФМЕТИКИ**

(57) Формула полезной модели

Вычислительный элемент бимодульной модулярной арифметики, содержащий устройство управления, оперативное запоминающее устройство (ОЗУ), постоянное запоминающее устройство (ПЗУ), мультиплексор, отличающийся тем, что в состав вычислительного элемента введен арифметический узел, реализованный с помощью пяти мультиплексоров, двоичного сумматора, двух преобразователей «минус единица», преобразователя «минус p», преобразователя «минус (p-1)», компаратора, логического блока, ПЗУ для хранения таблицы бимодульной пары, блока выходных регистров, причем выход устройства управления соединен с четвертым входом логического блока, управляющим входом ПЗУ для хранения таблицы бимодульной пары и управляющими входами первого, второго, четвертого и пятого мультиплексоров арифметического узла, сигнал с первого мультиплексора поступает соответственно на вход первого преобразователя «минус единица», первый вход двоичного сумматора и второй вход логического блока, сигнал со второго мультиплексора поступает соответственно на вход второго преобразователя «минус единица», второй вход двоичного сумматора и третий вход логического блока, выход первого преобразователя «минус единица» соединен с первым информационным входом третьего мультиплексора, выход второго преобразователя «минус единица» соединен с восьмым информационным входом третьего мультиплексора, выход двоичного сумматора соединен с входом преобразователя «минус p», входом преобразователя «минус (p-1)», пятым информационным входом третьего мультиплексора и входом компаратора, выход преобразователя «минус p» соединен с третьим информационным входом третьего мультиплексора, выход преобразователя «минус (p-1)» соединен с четвертым информационным входом третьего мультиплексора, а на второй, шестой и седьмой информационные входы третьего мультиплексора поступают константные значения.

Стр. 1

Последний из патентов В. М. Амербаева

5

О МАТЕМАТИЧЕСКОЙ СПЕЦИФИКАЦИИ УНИВЕРСАЛЬНОГО ГЕНЕТИЧЕСКОГО КОДА.

В.М.Амербаев
Институт теоретической и прикладной математики МН-АН РК

1. УГК.

Генетический код - основной закон молекулярной биологии, который устанавливает правила трансляции последовательности нуклеотидов РНК в аминокислотную последовательность белков.

При этом [1]: каждый триплет РНК определяет включение в аминокислотную последовательность только одной аминокислоты; рамка считывания информации, записанной в РНК, устанавливается при инициации трансляции и сохраняется на протяжении всего процесса; так как РНК является линейным полимером, состоящим из нуклеотидов четырех типов (A - аденин, G - гуанин, C - цитизин, U -урацил), то множество всех возможных триплетов $G(4^3)$ состоит из 64 различных элементов; так как множество A всех аминокислот, которые микробиологи находят в белках, состоит из 20 различных аминокислот, то генетический код вырожден; генетический код (см. табл.1) чрезвычайно консервативен в эволюции, за небольшим исключением он остается одинаковым у таких разных организмов, как бактерии, растения и человек, поэтому этот код принято называть универсальным генетическим кодом (УГК).

Если расширить множество A символом "стоп", который отвечает трем триплетам, играющим роль терминальных стоп-сигналов при трансляции, то УГК в математических терминах приобретает смысл сюръективного отображения: $G(4^3) \xrightarrow{УГК} \{AU"стоп"\}$, причем разбиение $G(4^3)$ на группы вырожденности представляет собой факторизацию $G(4^3)$ по данному отображению УГК.

Цель данной статьи - дать математическую спецификацию УГК, в которой нашли бы отражение существенные свойства УГК. При этом основной акцент делается на свойство непрерывности вырожденности, как некого инварианта УГК. В этом отличие в данной системе подхода к математическому описанию УГК от подходов, использованных в работах [2, 3].

6

Таблица 1. УГК

	U	C	A	G	
	0 Phe	4. Ser	8. Tyr	12. Cys	U
U	1. Phe	5. Ser	9. Tyr	13. Cys	C
	2. Leu	6. Ser	10. Стоп	14. Стоп	A
	3. Leu	7. Ser	11. Стоп	15. Trp	G
	16. Leu	20. Pro	24. His	28. Arg	U
C	17. Leu	21. Pro	25. His	29. Arg	C
	18. Leu	22. Pro	26. Gln	30. Arg	A
	19. Leu	23. Pro	27. Gln	31. Arg	G
	32. lie	36. Thr	40. Asn	44. Ser	U
A	33. lie	37. Thr	41. Asn	45. Ser	C
	34. lie	38. Thr	42. Lys	46. Arg	A
	35. Met	39. Thr	43. Lys	47. Arg	G
	48. Val	52. Ala	56. Asp	60. Gly	U
G	49. Val	53. Ala	57. Asp	61. Gly	C
	50. Val	54. Ala	58. Glu	62. Gly	A
	51. Val	55. Ala	59. Glu	63. Gly	G

Известна [4] естественно-научная интерпретация вырожденности УГК, которая гласит, что избыточность кодонов, обусловленная вырожденностью УГК, связана с частотой встречаемости соответствующих аминокислот в белках живых организмов: в некоем расплывчатом смысле справедливо - чем больше частота встречаемости аминокислоты, тем больше степень вырожденности (число кодонов) соответствует ей, следствием чего является более высокая помехозащищенность аминокислоты в белковой последовательности от мутаций на уровне ДНК(РНК). Но вырожденность имеет, по-видимому, более тонкую биологическую и структурно-химическую смысловую нагрузку. В частности, она играет фундаментальную роль в так называемой нейтральной теории [4]. Поэтому актуальность проблемы математической спецификации УГК очевидна.

УГК наделен лексико-графическим порядком. Начальным элементом является первый кодон (U, U, U) аминокислоты Phe. Этот порядок закреплен свойством непрерывности вырожденности: каждая группа вырожденности состоит из рядом перечисленных кодонов соответствующей аминокислоты:

7

Таблица 2. Сегменты непрерывности вырожденности

Имя аминокислоты	символ	степень вырожден-ности	сегменты вырожденност
1. Фенилаланин	Phe	2	[0,1]
2. Лейцин	Leu	6	[2,3], [16,17,18,19]
3. Серин	Ser	6	[4,5,6,7], [44,45]
4. Тирозин	Tyr	2	[8,9]
5. Цистеин	Cys	2	[12,13]
6. Триптофан	Trp	1	[15]
7. Пролин	Pro	4	[20,21,22,23]
8. Гистедин	His	2	[24,25]
9. Глутамин	Gln	2	[26,27]
10. Аргинин	Arg	6	[28,29,30,31],[46,47]
11. Изолейцин	Ile	3	[32,33,34]
12. Метионин	Met	1	[35]
13. Треонин	Thr	4	[36,37,38,39]
14. Аспоргин	Asn	2	[40,41]
15. Лизин	Lys	2	[42,43]
16. Валин	Val	4	[48,49,50.51]
17. Аланин	Ala	4	[52,53,54,55]
18. Аспоргиновая кислота	Asp	2	[56,57]
19. Глутаминовая кислота	Glu	2	[58,59]
20. Глицин	Gly	4	[60,61,62,63]
21. Стоп-сигнал.	Стоп	3	[10,11], [14]

В таблице 2 аминокислоты расположены в том порядке, в котором они представлены в УГК. Назовем этот порядок каноническим. Канонический порядок находит отражение в порядке следования сегментов вырожденности. Однако, Leu, Ser, Arg имеет разнесенные друг относительно друга сегменты непрерывности. Назовем упорядоченную последовательность сегментов зафиксированную законом УГК - конфигурацией вырожденности аминокислот. Очевидно, что канонический порядок и конфигурация вырожденности инварианты

8

2. Математическая модель УГК.

Возникают первые вопросы: имеется ли какое-либо объяснение тому, что число терминальных триплетов равно 3 и что число кодонов с вырожденностью 1 равно 2 (это Trp и Met). Известно, что кодон Met играет роль стартового сигнала: любая белковая цепочка начинается с метионина (Met). Каков же смысл кодона Trp? Известно лишь [5], что частота встречи Trp в живых организмах реже, чем у Met. Поиск ответов на поставленные вопросы приводит к новой математической интерпретации УГК.

Если исключить из рассмотрения три терминальных стоп-сигнальных триплета, то оставшиеся 61 триплета являются кодонами (смысловыми триплетами).

Число 61 является простым в кольце Z целых чисел, но не является таковым в кольце целых гауссовых чисел CZ. Здесь оно разлагается на попарно-сопряженные комплексные числа: $61 = 6^2+5^2 = (6+5i)(6-5i) = (-5+6i)(-5-6i) = (-6+5i)(-6-5i) = (5+6i)(5-6i)$. Отношения делимости, порожденные делимостью гауссовых чисел по перечисленным модулям (числам), разбивает целочисленную сетку (кольцо) CZ на конгруэнтные квадраты такие, что каждое гауссово число, попавшее в тот или иной квадрат, сравнимо по соответствующему модулю с единственным вычетом из класса вычетов [6]. Из всех возможных классов вычетов по перечисленным модулям выберем такие, которые образуют хиральную пару.

Определение. Два класса вычетов CZ_p^- и CZ_p^+ по перечисленным модулям образуют хиральную пару, если они зеркально симметричны относительно биссектрисы первого координатного угла и не имеют общих точек кроме нуля. Хиральные пары, например, образуют полные системы наименьших неотрицательных вычетов CZ_{6+5i}^+ и CZ_{-6+5i}^-. Полные системы абсолютно наименьших вычетов CZ_{6+5i}^- и CZ_{-6+5i}^- и другие не могут образовывать хиральные пары, так как нарушается второе условие определения хиральности.

Возьмем за основу кольцо CZ_{6+5i}^+, которое состоит из чисел:

CZ_{6+5i}^+ := {5+4i, 6+4i; 4+3i, 5+3i, 6+3i, 6+3i, 7+3i; 3+2i, 4+2i, 5+2i, 6+2i, 7+2i, 8+2i; 2+i, 3+i, 3+i, 4+i, 5+i, 6+i, 7+i, 8+i, 9+i; 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10; 1-i, 2-i, 3-i, 4-i, 5-i, 6-i, 7-i, 8-i, 9-i, 10-i; 2-2i, 3-2i, 4-2i, 5-2i, 6-2i, 7-2i, 8-2i, 9-2i; 3-3i, 4-3i, 5-3i, 6-3i, 7-3i, 8-3i; 4-4i, 5-4i, 6-4i, 7-4i; 5-5i, 6-5i}.

Поставим задачу: уложить 61 смысловой кодон в CZ_{6+5i}^+ так, чтобы при этом сохранить канонический порядок конфигурации и непрерывность вырожденности УГК.

9

Простой перебор всех возможных цикличных сдвигов показал, что поставленную задачу решает единственная укладка, которая удовлетворяет теореме Гаусса [6] об изоморфизме кольца вещественных неотрицательных вычетов по mod 61 кольцу комплексных неотрицательных вычетов по mod (6+5i) при единственном условии, что нумерация смысловых кодонов начинается с кодона Trp. Результаты укладки сведены в таблицу 3.

Таблица 3.

Trp	0+0i	0	0	(0,0)	Met	9+i	20	40	(8,10)
	1+0i	1	1	(1,1)		4-4i	21	41	(9,1)
Leu	2+0i	2	2	(2,2)	Thr	5-4i	22	42	(10,2)
	3+0i	3	3	(3,3)		6-4i	23	43	(11,3)
	4+0i	4	4	(4,4)		7-4i	24	44	(12,4)
	5+0i	5	25	(5,5)					
Pro	6+0i	6	26	(6,6)	Asn	3+2i	25	5	(1,5)
	7+0i	7	27	(7,7)		4+2i	26	6	(2,6)
	8+0i	8	28	(8,8)					
His	9+0i	9	49	(9,9)	Lys	5+2i	27	7	(3,7)
	10+0i	10	50	(10,10)		6+2i	28	8	(4,8)
Gin	5-5i	11	51	(11,1)	Ser	7+2i	29	29	(5,9)
	6-5i	12	52	(12,2)		8+2i	30	30	(6,10)
	2+i	13	13	(1,3)					
Arg	3+i	14	14	(2,4)	Arg	3-3i	31	31	(7,1)
	4+i	15	15	(3,5)		4-3i	32	32	(8,2)
	5+i	16	16	(4,6)					
	6+i	17	37	(5,7)		5-3i	33	53	(9,3)
lie	7+i	18	38	(6,8)	Val	6-3i	34	54	(10,4)
	8+i	19	39	(7,9)		7-3i	35	55	(11,5)
						8-3i	36	56	(12,6)

10

	4+3i	37	17	(1,7)				
Ala	5+3i	38	18	(2,8)	Leu	1-i	51	11	(3,1)
	6+3i	39	19	(3,9)		2-i	52	12	(4,2)
	7+3i	40	20	(4,10)					
						3-i	53	33	(5,3)
Asp	2-2i	41	21	(5,1)	Ser	4-i	54	34	(6,4)
	3-2i	42	22	(6,2)		5-i	55	35	(7,5)
						6-i	56	36	(8,6)
Glu	4-2i	43	23	(7,3)	Tyr	7-i	57	57	(9,7)
	5-2i	44	24	(8,4)		8-i	58	58	(10,8)
	6-2i	45	45	(9,5)					
Gly	7-2i	46	46	(10,6)	Cys	9-i	59	59	(11,9)
	8-2i	47	47	(11,7)		10-i	60	60	(12,10)
	9-2i	48	48	(12,8)					
Phr	5+4i	49	9	(1,9)					
	6+4i	50	10	(2,10)					

Таблица 3 состоит из двух столбцов каждый из которых разбит на 5 подстолбцов. Первый из них содержит имена аминокислот, начиная с Trp в том порядке, как они заданы в УГК, второй подстолбец - их комплекснозначные значения, третий подстолбец - номер аминокислоты, который предвычисляется по формуле теоремы Гаусса об изоморфизме $r=|x+\rho y|_{61}$ с коэффициентом изоморфизма равным $\rho = 11$, четвертый подстолбец содержит сегменты теневой (дуальной) вырожденности УГК (смотри об этом ниже); пятый подстолбец - модулярный код [7] для аминокислот по паре избыточных модулей (12, 10), который ярко выражает циклы УГК с периодами 12 и 10. Ясно, что наблюдаемые циклы УГК обусловлены природой мультипликативной группы кольца наименьших неотрицательных вычетов CZ^{+}_{6+5i}. Любопытен следующий факт: представим себе любое распределение порядка следования аминокислот, обладающее свойством непрерывной вырожденности и вложимости смысловых кодонов в CZ^{+}_{6+5i}. Оказывается, ля него всегда существует (и притом единственная) укладка в CZ^{+}_{6+5i} вырожденности с сохранением прежней конфигурации, однако с

новыми номерами кодонов соответствующих аминокислот. Для канонической таблицы УГК этот факт отражен в четвертом столбце.

3. Выводы

Предложенная спецификация УГК обладает следующими свойствами:

3.1. Вырожденность УГК вложима в структуру мультипликативной группы CZ^{+}_{6+5i} без нарушения непрерывности вырожденности и вложимость единственна, начинается она с кодона Trp.

3.2. Существует теневая (дуальная) вложимость вырожденности без нарушения конфигурации и непрерывности вырожденности, которая получается из исходного порядка аминокислот соответствующей перестановкой.

3.3. Поскольку система вычетов CZ^{+}_{6+5i} хиральна системе CZ^{+}_{-6+5i} то кодон Trp наделяется двумя свойствами: он является аддитивным нейтральным элементом кольца вычетов и его хиральность определяет хиральность всех остальных кодонов (элементов рассматриваемого кольца вычетов)

ЛИТЕРАТУРА

1. Альбертс, Д. Брей, Дж. Льюис, М. Рэфф, К. Робертс, Дж. Уотсон. "Молекулярная биология клетки" // т.1. М. Мир. 1994
2. Щербак. "Математическая модель универсального гинетического кода" (автореферат диссертации) // Алматы. 1995
3. MilojeM Rakocevic. " Logic of The Genetic Code" // Научик Дыма, Beograd. 1994
4. Jukes. "Nutrition Science From Vitamins to Molecular Biology" // Annual Review of Nutrition. vol.10. 1990
5. Льюин. "Гены" // М. Мир. 1990
6. Амербаев, И.Т. Пак. "Параллельные вычисления в комплексной плоскости" // Алма-Ата. Наука. 1984
7. Амербаев. "Теоретические основы машинной арифметики" // Алма-Ата. Наука. 1976.

Опубликовано в сборниках:

- *Доклады Министерства науки — Академии наук Республики Казахстан (ДАН РК). — №5, Алматы, 1996 г. — С. 22–28.*
- *Динамический хаос в распределённых системах. — Вып. 1. — Институт теоретической и прикладной математики Министерства науки — Академии наук РК. Препринт 50 экз. 1996. — С. 5—11.*

Модулярной арифметике — 50 лет

Амербаев В. М., Пак И. Т.

Рассмотрена краткая история зарождения и развития системы счисления остаточных классов (модулярной арифметики). Показано, что современные модели компьютерных арифметик по своей природе являются архимедовыми. Дан анализ понятия «модулярная арифметика». Её перспективу составляет разработка различных приёмов комплексирования (сближения) достоинств позиционной и модулярной арифметик в целях достижения сверхпроизводительности и сверхнадёжности вычислительных структур, спроектированных на элементной базе, предельно реализующих возможности технологии.

Прошло 50 лет с тех пор, как чешский учёный-инженер Миро Валах (в 1955 году) предложил для кодирования целых чисел в математических машинах использовать кольцо вычетов по составному модулю с попарно взаимнопростыми основаниями. После первых публикаций Антонина Свободы и Миро Валаха (1955 г.) эта идея была с энтузиазмом подхвачена мировой научной общественностью в области компьютерных технологий (в большей степени — американской), и к 1959 году из открытых публикаций можно было получить достаточно чёткое представление о базовых принципах конструирования модулярной арифметики, её достоинствах и недостатках. Сформировалось новое движение научной мысли в науке о вычислениях и о компьютерной арифметике. Начальные вехи этого движения за рубежами СССР таковы:

- Свобода и Валах (1954–1958 гг. [1–6]) исследовали базовые свойства арифметики в остатках (модулярной арифметики);
- Айкен и Семон (1959 г. [7–8]) показали преимущества модулярной арифметики;
- Гарнер (1959 г. [9–10]) исследовал арифметические свойства модулярной арифметики в целях построения самокорректирующихся арифметичных кодов, исследовал принципы синтеза систем счисления;

- Чини (1961 г. [11]) сконструировал цифровой коррелятор в остатках;
- Сабо (1962 г. [12]) доказал, что знак любого числа в остаточных кодах является функцией всех остатков (что, собственно, сродни свойству самокоррекции кодов в остатках, основанной на высокой чувствительности этих кодов к малейшему изменению любого остатка по любому основанию);
- Шапиро (1964 г. [13]) исследовал принципы организации параллельных вычислений в модулярной арифметике.

В последующем количество работ в области модулярной арифметики нарастало, как снежный ком.

В Советском Союзе первая открытая публикация по модулярной арифметике состоялась в 1964 году в широко известном сборнике переводов под редакцией А. А. Ляпунова и О. Б. Лупанова — «Кибернетический сборник», № 8 — серией статей ведущих зарубежных специалистов в области модулярной арифметики.

Далее:

- Андрианов Е. С. (1964 г. [14, 15]) исследовал вопросы реализации важнейших немодульных операций;
- Акушский И. Я., Юдицкий Д. И. Машинная арифметика в остаточных классах. — М., 1968 (популярная в России монография);
- Торгашов В. А. Система остаточных классов и надёжность ЦВМ — М., 1973 (известная в России монография).

Однако значительно раньше упомянутого выше «Кибернетического сборника» работы в области модулярной арифметики в СССР были начаты группой учёных и инженеров — И. Я. Акушским, Д. И. Юдицким, Е. С. Андриановым, перед которыми была поставлена задача разработать модулярный процессор [27]. Результатами теоретических исследований и практического использования стала докторская диссертация И. Я. Акушского и кандидатские диссертации Д. И. Юдицкого и Е. С. Андрианова, защищённые в 1964–1965 годах, а также модулярные ЭВМ Т-340А (экспериментальная) и К-340А (производилась серийно).

В 1964 г. возглавляемый Д. И. Юдицким и И. Я. Акушским коллектив приверженцев модулярной арифметики переместился в создаваемый тогда Центр микроэлектроники в Зеленограде. На базе этого коллектива был образован Специализированный вычислительный центр (СВЦ) с задачей создания высокопроизводительной модулярной ЭВМ 5Э53 [27].

Публикация работ в «Кибернетическом сборнике», а затем монографии Акушского И. Я. и Юдицкого Д. И. стимулировали независимые исследования в конце 1960-х гг.: в Ленинграде — Торгашов В. А.; В Киеве — Вышенский В. А., Мороз И. Г., Петушак В. Д.; в Алма-Ате — Амербаев В. М., Пак И. Т., Казангапов А. Н., Бияшев Р. Г.; в Тбилиси — Хацкевич В. Х.; в Минске — Коляда А. А. и Чернявский А. Ф., активно развивающие оригинальные идеи в области модулярных вычислений по настоящее время.

В семидесятых и последующих годах высокий имидж модулярной арифметики в Союзе (вне стен СВЦ) поддерживался блестящим талантом И. Я. Акушского, увлёкшего идеями модульной арифметики молодых учёных и приобщившего их к разработкам в этой области. Не имея возможности встречаться с молодыми «соковцами» в стенах закрытого учреждения (СВЦ), он широко открыл перед ними двери своей квартиры, где Галина Петровна (жена Израиля Яковлевича) и Елизавета Соломоновна (мать его жены) радушно встречали всех посетителей. Трудно представить себе личностное влияние И. Я. Акушского на развитие модулярной арифметики в Союзе без тёплого и внимательного соучастия его семейного окружения. В последующем очаги модульной арифметики возникли в Нижнем Новгороде, Ставрополе, Воронеже, Харькове, Днепропетровске, Дагестане. Были созданы новые большие школы, возглавляемые Чернявским А. Ф. и Колядой А. А., Червяковым Н. И., Краснобаевым В. А. и др.

Несмотря на столь широкое распространение модулярной арифметики в технике вычислений, само понятие «модулярная арифметика» заслуживает более подробного анализа. Мы настолько привыкли к позиционной арифметике, что понятие «позиционный код» отождествляется нами с понятием числа.

В действительности это не так. Дело в том, что в понятии числа присутствует некая тройственность:

- число как некий объект (возникший исторически в результате осмысления таких процессов человеческой деятельности, как счёт и измерение),
- способ представления числа, т. е. синтаксис объекта,
- смысл числа (количество, величина), т. е. семантика объекта.

Семантика числа в полной мере отражается системой аксиом вещественных чисел **R.**

Как известно, таких аксиоматик, дающих полное описание понятия числа, несколько: дедекиндова, канторова, вейерштрассовская:

- вейерштрассовская трактовка числа существенно использует позиционное представление чисел, тем самым, как бы универсализируется сам факт позиционного представления чисел;
- канторова трактовка базируется на плотности рациональных чисел **Q** в **R** или, точнее, на пополнении **Q** до **R**;
- дедекиндово понимание числа эксплуатирует факторизацию — разбиение **Q** на классы эквивалентности, так называемые сечения Дедекинда.

Все эти аксиоматики порождают (с точностью до изоморфизма, и это доказано) одно и то же множество объектов, называемых числами. Тем самым показано, что позиционное представление числа равнозначно всем другим средствам описания чисел. Требования к способу представления чисел чётко определены Леонардом Эйлером: «Всякий способ изображения чисел требует к арифметическим действиям особых правил, которые подлежит производить от свойств оных чисел, кои употребляются» [28]. Эйлеровские требования к способу изображения чисел можно рассматривать как научную программу построения компьютерных моделей чисел. Как следует из аксиоматического определения числа, целые числа составляют конструктивную основу, с помощью которых строятся вещественные числа. Понятие же целого числа возникло в результате практики счёта. «Все числа, как ты знаешь, состоят из некоторого количества

единиц» (Диафант). Целые числа образуют бесконечное упорядоченное кольцо, базовые операции которого (сложение, вычитание, умножение) согласованы с отношением естественного порядка чисел. С помощью целых чисел (т. е. пар целых чисел) определяется также понятие дробного (рационального) числа. Необходимость в определении множества рациональных чисел возникла в результате обобщения измерительных процессов. Опыт измерений отражён в так называемой аксиоме Архимеда, которая в наиболее рафинированной форме формулируется следующим образом: «Любое вещественное число x единственным образом представимо в виде суммы целой части числа, обозначим её временно символом $W(x)$, и дробной части того же числа, обозначим её символом $f(x)$»:

$$\forall x \in R \quad \exists! \quad W(x) \in Z; \quad x = W(x) + f(x).$$

Наибольшее распространение имеют два случая выбора дробной доли:

• наименьшая неотрицательная дробная часть, т. е.

$$0 \le f(x) < 1 \quad \forall x \in R,$$

этот случай соответствует экстремальному выбору целой части как наибольшего целого числа, не превосходящего x; такую целую часть принято обозначать символом $\lfloor x \rfloor$ [16];

• абсолютно наименьшая дробная часть:

$$-\frac{1}{2} \le f(x) < \frac{1}{2} \quad \forall x \in R,$$

которая соответствует экстремальному выбору целой части как ближайшего к x целого числа: такую целую часть принято обозначать символом $\lfloor x \rceil$ [16].

Итак, аксиома Архимеда записывается в двух формах и утверждает она единственность разложений вида

$$\forall x \in R \quad \exists! \quad \lfloor x \rfloor \in Z: \quad x = \lfloor x \rfloor + f(x),$$

где $0 \le f(x) < 1$,

$$\forall x \in R \quad \exists! \quad \lfloor x \rfloor \in Z: \quad x = \lfloor x \rceil + f^{-}(x),$$

где $-\frac{1}{2} \le f^{-}(x) < \frac{1}{2}$.

Связь между этими двумя разложениями устанавливается соотношениями

$$\lfloor x \rceil + \left\lfloor x + \frac{1}{2} \right\rfloor, \quad f^{-}(x) = f\left(x + \frac{1}{2}\right) - \frac{1}{2}.$$

Из аксиомы Архимеда следует, что любое вещественное число с любой наперёд заданной точностью может быть приближено рациональным числом.

Пусть M — достаточно большое число (натуральное), тогда

$$\forall x \in R \quad Mx = \lfloor Mx \rceil + f^{-}(Mx) \text{ или } x = \frac{1}{M}\lfloor Mx \rceil + \frac{f^{-}(Mx)}{M},$$

отсюда следует, что абсолютная величина ошибки представления числа x дробью $\lfloor Mx \rceil / M$ не превышает величины $\frac{1}{2M}$. Величина M называется масштабным множителем. Если M — постоянный масштаб, то представление чисел x дробями вида $\lfloor Mx \rceil / M$ имеет равномерно распределённую абсолютную ошибку, что удобно для больших значений x и неудобно для малых. Для того чтобы устранить этот недостаток режима фиксированной запятой, вводят понятие относительной погрешности. Требуется, чтобы уже относительная, а не абсолютная ошибка представления вещественных чисел рациональными была равномерно распределённой. Это требование обусловливает введение переменного масштабного множителя и соответствующего представления чисел с плавающей запятой. Теперь абсолютная ошибка растёт с увеличением числа x. Балансирование между этими представлениями чисел определяется стратегией вычислений и относится к категории метатеории вычислений (т. е. семантики вычислений). Важно отметить, что масштабирование регулирует информационную ёмкость представления чисел рациональными дробями.

Из сказанного следует, что если строить модели компьютерных чисел, то в первую очередь необходимо построить модель арифметики целых чисел и далее, используя принцип масштабирования, добиваться нужных точностных характеристик. Этот вывод касается, так сказать, семантического, т. е.

метрического, количественного, точностного аспекта представления чисел, тогда как реализация арифметических операций связана со способом кодирования (т. е. изображения) чисел. Как будет показано ниже, реализация арифметических операций также связана с масштабирующими множителями, но уже не столько с их величинами, сколько с их структурной (мультипликативной) характеристикой. Варьируя величину и структуру масштабирующих множителей, можно получить разнообразные структуры компьютерных арифметик. Современные технологии проектирования вычислительных средств на различной элементной базе микроэлектроники позволяют адаптировать вычислительные среды к различным арифметическим структурам в целях эффективного сочетания таких показателей вычислительных процессов, как точность, параллелизм, надёжность, реконфигурируемость и т. п. В этом смысле чем богаче набор различных арифметических структур, тем более успешно может быть решена проблема оптимизации вычислений при решении того или иного класса задач на данной вычислительной среде или данной элементной базе.

Возвращаясь к вопросу о компьютерной модели целых чисел Z, следует заметить, что сама модель должна быть конечной, должна максимально точно представлять все арифметические операции над целыми числами и сохранять естественный порядок целых чисел.

Наилучшим образом такая модель, состоящая из N элементов, представляется набором целых чисел полной системы абсолютно наименьших вычетов множества целых чисел Z по модулю N:

$$Z_N^- = \left\{ x \in Z \,|\, -\frac{N}{2} \le x < \frac{N}{2} \right\}.$$

В ряде случаев по чисто техническим причинам бывает удобно за конечную модель принять наименьшие неотрицательные вычеты по модулю N, т. е.

$$Z_N = \{ x \in Z \,|\, 0 \le x < N \}.$$

При построении колец Z_N^- и Z_N, имитирующих на компьютерном уровне кольцо Z, мы вновь не обходимся без аксиомы Архимеда. Действительно, согласно аксиоме Архимеда справедливо

$$\forall x \in Z \quad \frac{x}{N} = \left\lfloor \frac{x}{N} \right\rfloor + f\left(\frac{x}{N}\right),$$

отсюда

$$\forall x \in Z \quad x = \left\lfloor \frac{x}{N} \right\rfloor N + f\left(\frac{x}{N}\right) N.$$

Так как $x, \left\lfloor \frac{x}{N} \right\rfloor N \in Z$, то $f\left(\frac{x}{N}\right) N \in Z$. Обозначим это целое число символом

$$|x|_N := f\left(\frac{x}{N}\right) N.$$

В теории чисел величина $|x|_N$ называется наименьшим неотрицательным вычетом целого числа x по модулю N. Область значений функции $y = |x|_N$ составляет числа $\{0, 1, 2, \ldots, N-1\}$. Это множество является кольцом наименьших неотрицательных вычетов по модулю N и обозначается символом Z_N, имеет кольцевые операции $\oplus, \otimes$, определяемые следующим образом:

$$\forall x, y \in Z_N \quad x \oplus y := |x + y|_N,$$

$$x \otimes y := |x \cdot y|_N.$$

Функция $y = |x|_N$ определена на Z и называется функцией вычетов по модулю N.

Пусть $|x|_N = r \quad r \in Z_N$.

Очевидно, что целые числа $z \in Z_N$ вида $z = r + kN \; \forall k \in Z$ отображаются функцией вычета в точку r. Множество всех этих целых чисел называется классом вычетов и обозначается как (r):

$$(r) = \{z \in Z \mid z = kN + r, \forall k \in Z\}.$$

Два числа $\forall z_1, z_2 \in Z$, принадлежащие одному классу вычетов, называются сравнимыми по модулю N, что записывается следующим образом: $z_1 \equiv z_2 (\mathrm{mod}\, N)$.

Таким образом, сравнение $z_1 \equiv z_2 (\mathrm{mod}\, N)$ равносильно двум равенствам:

$(z_1) = (z_2)$ — равенство классов вычетов по модулю N,

$|z_1|_N = |z_2||_\Lambda$ — равенство вычетов чисел z_1 и z_2 по модулю N.

Множество всех классов вычетов по модулю N обозначается символом $Z/(N)$ и называется фактор-кольцом кольца Z по модулю N. Оно изоморфно кольцу вычетов Z_N; пишут $Z/(N) \cong Z_N$.

Таким образом, с функцией вычетов связана следующая схема гомоморфных (т. е. сохраняющих кольцевые свойства) отображений (рис. 1).

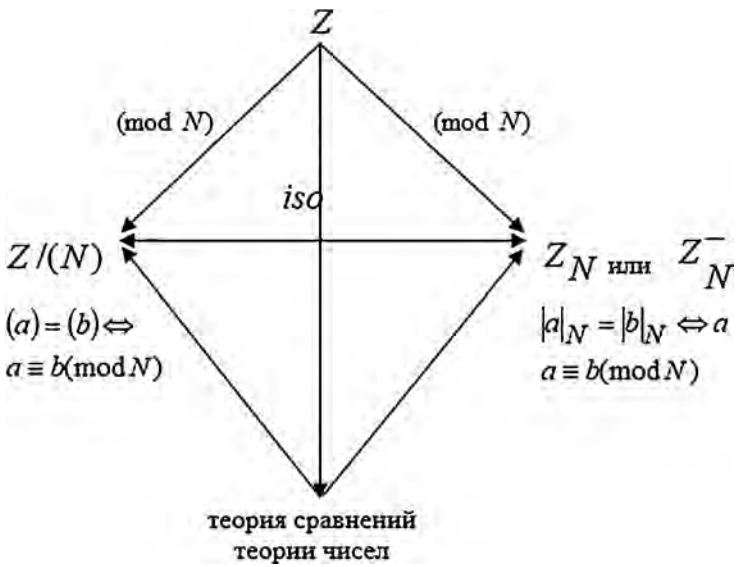


Рис. 1. Схема гомоморфных отображений

При этом только правая ветвь $Z \to Z_N$ отвечает требованиям, сформулированным Л. Эйлером к конструированию конечной модели кольца Z.

Из этой схемы явно просматривается неточность термина «система счисления остаточных классов», идущая

от А. Свободы [4], т. к. «остаточные классы» или «классы вычетов» образуют элементы фактор-кольца $Z/(N)$, тогда компьютерная модель целых чисел является кольцом вычетов (остатков) Z_N. Возможно, этой замысловатости термина СОК мы обязаны тому, что один из ведущих в Союзе разработчиков ЭВМ М. А. Карцев в своей книге [17] назвал СОК «экзотической системой счисления» и тем самым углубил недопонимание значимости модулярной арифметики у многих разработчиков вычислительных средств.

В действительности никакой экзотичности нет. Модулярная арифметика, как и всякая другая компьютерная арифметика, на регистровом уровне является кольцом вычетов Z_N, что существенно важно, т. к., во-первых, Z_N образует отрезок из множества Z, точнее, подмножество множества Z, непосредственно идущих друг за другом в порядке возрастания целых чисел, общее количество которых равно N, во-вторых, указана связь между моделируемыми арифметическими операциями над целыми числами и их модельными аналогами (кольцевыми операциями), которая выражается следующим утверждением: для любых $x, y \in Z_N$ имеют место равенства

$$x + y = |x + y|_N,\ x \cdot y = |x \cdot y|_N$$

тогда и только тогда, когда результаты соответствующих арифметических операций +,• над вычетами, как целыми числами, не выходят за «диапазон» $Z_N = \{x \in Z \mid 0 \le x < N\}$. Последнее утверждение назовём условием согласования. Таким образом, любая компьютерная арифметика на регистровом уровне должна сопровождаться «мониторингом» условия согласования и, если это условие нарушается, система слежения должна соответствующим образом реагировать. Реакция зависит от режима вычисления: в целых числах или с дробями, с фиксированной или с плавающей точкой, в режиме обнаружения и исправления ошибок и т. п. Здесь умышленно использовано слово «мониторинг», чтобы подчеркнуть фундаментальность этой операции в сигнатуре любой компьютерной модели чисел, часто опускаемой «по умолчанию».

Таким образом, компьютерная модель целых чисел — это арифметика кольца вычетов по некоторому модулю N плюс мониторинг условия согласования. Сам мониторинг реализуется опять же посредством аксиомы Архимеда. Например, если контролируется выход результата аддитивной операции за диапазон, то этот контроль осуществляется функцией

$$\eta = \left\lfloor \frac{x+y}{N} \right\rfloor = \begin{cases} 1 & \text{если} \quad x+y \notin Z_N \\ 0 & \text{если} \quad x+y \in Z_N \end{cases}.$$

Легко видеть, что указанный контроль не может быть осуществлён посредством модульных операций кольца вычетов Z_N, так как

$$\forall x, y \in Z : \left\lfloor \frac{|x+y|_N}{N} \right\rfloor = 0.$$

Иначе говоря, контроль аддитивного переполнения является немодульной операцией.

Отсюда, в частности, следует, что поскольку аксиома Архимеда является составной частью семантики вещественных чисел (т. е. всех аксиоматических систем **R**), то любая компьютерная модель чисел неизбежно является архимедовой и любые реальные вычисления с вещественными числами являются архимедовыми.

Многообразие компьютерных арифметик зависит от структуры модуля N и от способа масштабирования. Синтаксис компьютерной арифметики, т. е. её система правил, зависит только от выбора модуля N. Вообще говоря, следует отметить, что перечисленной выше спецификой компьютерной арифметики целых чисел обладают вычислительные структуры не только с числовым модулем N, но и с модулями более сложной природы (кольцо главных идеалов) [18]. Возвращаясь к числовому модулю N, отметим, что нетрудно установить связь между Z_N и Z_N^-:

$$\forall x \in Z \quad |x|_N^- = \left| x + \left\lfloor \frac{N}{2} \right\rfloor \right|_N - \left\lfloor \frac{N}{2} \right\rfloor.$$

Вывод. Всякая компьютерная арифметика целых чисел на регистровом уровне (будем говорить кратко «регистровая

арифметика») является модулярной, т. е. условно разбивается на модульную арифметику по модулю N регистра и систему мониторинга за переполнением результата вычислений за динамический диапазон регистра.

Далее, если всё сказанное выше характеризует смысл (семантику) регистровой арифметики, то вопросы кодирования её элементов относятся, так сказать, к синтаксису регистровой арифметики. Здесь уже существенное значение приобретает природа модуля N кольца вычетов [19].

При $N = 2^n$ имеет место двоичный код, при $N = 3^n$ — троичный, при $N = p_1, \ldots p_n$, где основания попарно взаимно просты — модулярный код (код в остатках). Кодирование вычетов называется позиционным, если лексикографический порядок этого кода совпадает с естественным порядком вычетов как целых чисел. В противном случае код называется непозиционным. Позиционному коду присуща простая организация мониторинга переполнения — сравнение чисел по величине, и более сложная — реализация арифметических операций над ними. Вычеты по составному модулю $N = p_1, p_2, \ldots p_n$ могут кодироваться двояко — позиционным (полиадический код), непозиционным (кодом в остатках); при этом непозиционный код эффективен в реализации операций кольца вычетов (модульные операции) и малоэффективен в процессах мониторинга переполнения (немодульные операции), а полиадический эффективен в процессах мониторинга и неэффективен в арифметических операциях кольца вычетов. Интерес к арифметике в остатках, которую только и принято называть модулярной арифметикой, вызван двумя обстоятельствами, присущими коду в остатках, — параллелизмом и свойством арифметической самокоррекции.

К настоящему времени с точки зрения современной технологии микроэлектроники и особенно технологии проектирования наиболее «обкатанной» является регистровая арифметика по модулю $N = 2^n$, т. е. двоичная арифметика. Немалый интерес представляет регистровая арифметика по модулю $N = 3^n$ [20]. Преимущественный интерес к этим видам арифметики при решении массовых задач обусловлен главным образом гибкостью

мониторинга условия согласования. При решении же некоторых типов индивидуальных задач (в специальных приложениях), когда возникает необходимость в получении на элементах «текущей технологии» такого сверхкачества на регистровом уровне, как повышение производительности средствами распределения и распараллеливания вычислительных нагрузок, повышение эксплуатационной надёжности средствами сочетания свойств арифметичной самокоррекции, реконфигурации и резервирования, преимущественный интерес приобретает модулярная арифметика. В связи с этим в разработках модулярной арифметики возникли две тенденции:

- привязка систем автоматизации проектирования, разработанной для двоичной арифметики, к задачам модулярной арифметики посредством адаптации модулей модулярной арифметики к удобному двоичному представлению [22], а также посредством сближения и комбинирования двоичной и модулярной арифметики [23],
- посредством разработки дополнительного программного обеспечения оптимального выбора модулей средствами целочисленного программирования, которые позволяют осуществить эффективную реализацию как модульных, так и немодульных операций.

Эти тенденции возникли ещё при проектировании ЭВМ 5Э53. Ярким примером тому служит программа, разработанная Я. Н. Кобринским, который решил задачу оптимального выбора модулей модулярной арифметики, удовлетворяющих техническим ограничениям. Эти ограничения описаны в работе [19] и связаны со специфическим видом модуля динамического диапазона и модуля избыточного диапазона, что обеспечивало возможность совмещения операции округления с операцией обнаружения и исправления ошибок, причём операция округления осуществлялась на основе алгоритма встречного расширения с использованием неточного ранга, позволяющего распараллелить операции встречного расширения. Таким образом, достигалась эффективная реализация операции округления, совмещённая с операцией обнаружения и исправления

ошибок, при вычислениях с дробями в режиме фиксированной запятой.

Как показал опыт проектирования 5Э53, успешная разработка модулярного процессора возможна только при слаженной, взаимодополняющей и взаимоувязанной работе большого коллектива технологов, схемотехников, программистов, математиков и при гибком централизованном управлении демократичным и энергичным архитектором проекта, таким, каким был Д. И. Юдицкий. Это объясняется тем, что в области проектирования модулярных процессоров до сих пор отсутствуют законченные рецепты и стандарты проектирования. Современные технологии микроэлектроники и технологии проектирования при соответствующей их адаптации могут с успехом использоваться при проектировании высокоэффективных модулярных процессоров, что, собственно, и составляет основу перспективного развития модулярной арифметики. Современная теория чисел способна за короткий срок дать ответы на все вопросы разработчиков, усилия которых направлены на сближение достоинств модулярной и двоичной арифметики и создания вычислительных структур и вычислительных сред двоично-модулярного типа на новых технологиях [21–27].

Модулярная арифметика заняла достойное место в теории вычислений, в компьютерной алгебре [30–34]. Как показывает обзор цитированных работ, перспективу модулярной арифметики представляют:

- теоретические исследования вопросов ускорения и повышения надёжности вычислений, связанные с выбором оснований арифметики в классе задач модулярной алгоритмики;
- создание вычислительных структур позиционно-модулярного типа, направленных на сближение достоинств модулярной и позиционной арифметики в целях комплексного достижения сверхпроизводительности и сверхнадёжности вычислений на современных вычислительных средствах, спроектированных на элементной базе, предельно реализующей возможности технологии:

- разработка интегрированных режимов варьирования масштабами вычислений;
- исследование и расширение классов задач, допускающих эффективную реализацию на гибридных модулярно-позиционных вычислительных средах.

Литература

1. Valach M. Vznik kodu a čiselene soustavy zbyitkovychtžid, Stroje na Zpracovani Informaci, Sbornik III, Praha, 1955, 211–255.
2. Valach M. Převodčiselze soustavy sbyitkovich třid do polyadicke soustavy změnon měřitka periody, Stroje na Zprancovani Informaci, Sbornik VI, Praha, 1956, 53–64.
3. Svoboda A., Valach M, Operatorove obovody, Stroje na Zpracovani Informaci, Sbornik III, Praha, 1955, 247–295.
4. Svoboda A. Rational numerical system of residual classes, Stroje na Zpracovani Informaci, Sbornik V, Praha, 1957, 9–37.
5. Svoboda A., The numerical system of residual classes in mathematical machines, Proc. Congreso Informational de Automatica, Madrid, October, 1958, 11–12.
6. Svoboda A., The numerical system of residual classes in mathematical machines, Information Progressing (Processings of UNESCO Conference, June, 1959) 1960, 419–422.
7. Aiken H. H. Theory of switching, Computation Lab., Harvard Univ., Cambrige., Mass. Rep N BL-23, June, 1959.
8. Aiken H. H., Semon W., Advanced Digital computer logic, WADC TR-59-472, July, 1959.
9. Garner H. L. Error checking and the structure of binary addition, Ph. D. Diss., Univ. Mitchigan, Ann Arbor, Mich., 1958.
10. Garner H. L., The residue number system, JRE Trans. On Electronic Computers, EC-8 (1959), June, 140–147.
11. Cheney P. W., A digital correlator based on the residue number system JRE Trans. on Electronic Computers, EC-10 (1961), March, 63–70.
12. Szabo N. Sign detection in non-redundant residue systems, JRE Trans. on Electronic Computers, EC-14 (1962), August, 494–501.

13. Shapiro H. S. Some remarks on Modular Arithmetics and Parallel Computation, Mathematics of computation (MTAC) v. 16, № 78, 1962, 218–222.
14. Андрианов Е. С. О методе определения знака в системе остаточных классов // Вопросы радиоэлектроники, 1964, серия XIII. — Вып. 2.
15. Андрианов Е. С. О некоторых методах организации округления в системе остаточных классов // Вопросы радиоэлектроники, 1964, серия XIII. — Вып. 8.
16. Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. — Вильямс: Москва — Санкт-Петербург — Киев, 2000.
17. Карцев М. А. Арифметика цифровых машин. — М., 1969.
18. Амербаев В. М. О построении систем счисления в остаточных классах в кольце главных идеалов // Труды М. О., 1967, № 75. — С. 61–81.
19. Амербаев В. М. Теоретические основы машинной арифметики — Алма-Ата: Наука, 1976. — 323 с.
20. Виноградов И. М. Основы теории чисел. — М., 1972.
21. Брусенцов Н. П. Вычислительная машина «Сетунь» Московского государственного университета // Новые разработки в области вычислительной математики и вычислительной техники. — Киев, 1960. — С. 226–234.
22. Стемпковский А. Л., Корнилов А. И., Семёнов М. Ю. Особенности реализации устройств цифровой обработки сигналов в интегральном исполнении с применением модулярной арифметики // Информационные технологии, 2004. — С. 2–8.
23. Евстигнеев В. Г. Недвоичная машинная арифметика и специализированные процессоры. — М.: МИФИ СЕРВИС и АО «ИНСОФТ», 1992.
24. Червяков Н. И., Сахнюк П. А., Шапошников А. В., Рядов С. А. Модулярные параллельные вычислительные структуры нейропроцессорных систем. — М.: Физматлит, 2003. — 288 с.

25. Инютин С. А. Модулярные вычисления в сверхбольших компьютерных диапазонах // Известия вузов. Электроника, 2001. — № 6. — С. 34–39.
26. Коляда А. А. Пак И. Т. Модулярные структуры конвейерной обработки цифровой информации. — Мн.: Университетское, 1992. — 256 с.
27. Малашевич Б. М., Малашевич Д. Б. Отечественные модулярные и троичные ЭВМ // Труды юбилейной Международной научно-технической конференции «50 лет модулярной арифметике». — Россия, Москва, Зеленоград, 23–25 ноября 2005. — М.: МИЭТ. — С. 101–148.
28. Л. Эйлер. Руководство к арифметике. Ч. 1. — СПб, 1740.
29. Малашевич Б. М., Малашевич Д. Б. Модулярная арифметика — взгляд изнутри // Труды юбилейной Международной научно-технической конференции «50 лет модулярной арифметике». — Россия, Москва, Зеленоград, 23–25 ноября 2005. — М.: МИЭТ. — С. 47–100.
30. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979.
31. Акпитас А. Основы компьютерной алгебры с приложениями. — М.: Мир, 1994.
32. Лидл Р., Пильц Г. Прикладная абстрактная алгебра. — Екатеринбург: изд. Уральского ун-та, 1996.
33. Глухов М. М., Елизаров Е. П., Нечаев А. А. Алгебра, Т. 1, 2. — М.: Гелиос АРВ, 2003.
34. Ноден П., Ките К. Алгебраическая алгоритмика. — М.: Мир, 1999.

Впервые опубликовано в трудах
юбилейной научно-технической конференции
«50 лет модулярной арифметики». —
М.: МИЭТ, 2005. — С. 5–21.

Система радиоуправления и радиомониторинга в подсистеме защиты информации глобальной системы спутниковой связи

Амербаев В. М., Любушкина (Грехнева) И.Е., Шарамок А. В.

Рассмотрена система радиоуправления и радиомониторинга средствами защиты информации абонентов глобальной системы спутниковой связи, решающая задачи ключевого обеспечения, мониторинга состояний средств защиты информации абонентов, дистанционного изменения работы средств защиты и сбора статистических данных.

Системы и услуги связи —одна из наиболее динамично развивающихся инфраструктур современного общества. Возникновение потребности в постоянной оперативной связи привело к интенсивному развитию и внедрению подвижных сетей (сотовых, транкинговых, персонального радиовызова) [1]. В связи с неудобством, возникающим при привязке абонента к конкретной области обслуживания, наблюдается процесс расширения зоны действия сетей. Некоторые специализированные службы и ведомства в настоящее время нуждаются в гарантированном и быстром предоставлении услуг связи независимо от географического местоположения абонентов. Подобные потребности помогают решить системы глобальной спутниковой связи (ГСС).

Основные характеристики таких систем связи: доступ к сети независимо от местоположения абонента, передача речевых, пейджинговых сообщений и пакетов данных, организация как индивидуальной, так и циркулярной связи, оперативное управление канальным ресурсом, возможность приоритетного выделения каналов связи.

Общая организация ГСС показана на рис. 1. Как правило, в ГСС присутствует космический

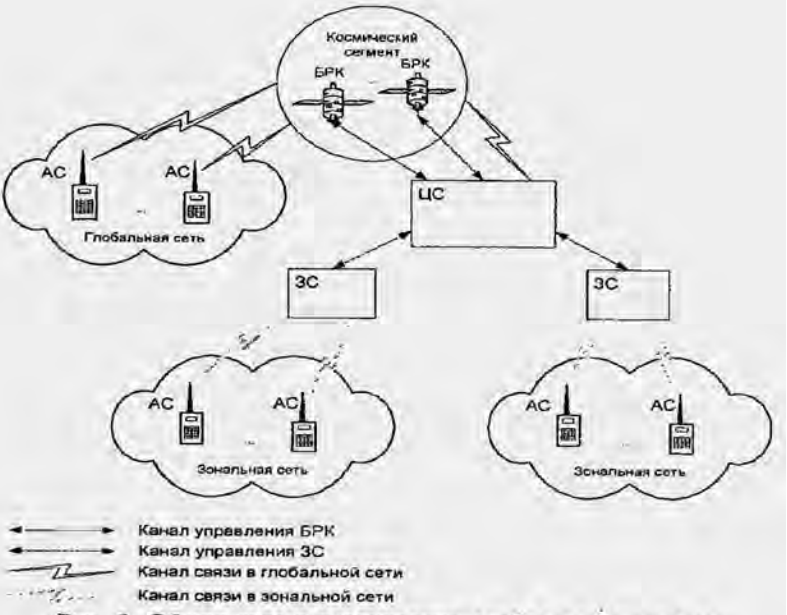


Рис. 1. Общая схема организации глобальной системы спутниковой связи

сегмент, центральная станция (ЦС), зональные станции (ЗС), и абоненты системы (абонентские станции — ЗС). Центральная станция занимается распределением канального ресурса, планированием связи, составлением расписаний, регистрацией абонентов и управлением всеми объектами системы. Зональная станция частично выполняет функции ЦС и организует зональные сети связи, также может выступать как абонент системы.

Информация, передаваемая через такие системы связи, как правило, носит конфиденциальный характер и должна подвергаться защите от несанкционированного ознакомления и навязывания ложных сообщений.

Для решения задач информационной безопасности на базе технических средств ГСС строится подсистема защиты информации, передаваемой по каналам связи. Возникает проблема

ключевого обеспечения абонентов системы, мониторинга состояния средств защиты, целенаправленного управления и изменения состояния в случае их некорректной работы. Данная проблема решается путем создания системы радиомониторинга и радиоуправления (СРР) средствами защиты информации (СЗИ) абонентов системы.

В задачи СРР входят:

- формирование ключевой информации для всех абонентов;
- рассылка ключей по каналам связи;
- сбор информации о текущем состоянии СЗИ абонентов;
- передача команд управления;
- ведение баз данных ключей и журналов событий безопасности.

Состав СРР представлен на рис. 2.

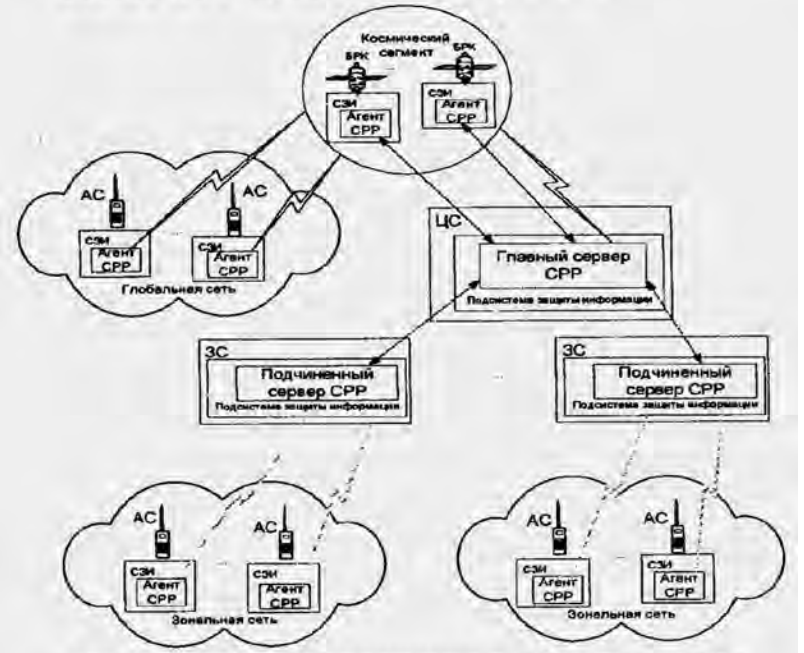


Рис. 2. Систе́ма радиоуправления и радиомониторинга подсистемы защиты информации в системе ГСС

Главный сервер СРР отвечает за формирование, рассылку, регламентную смену и уничтожение ключей, регистрацию абонента в системе безопасности, сбор информации о состоянии подсистемы безопасности, ведение баз данных и журналов, блокирование или разрешение работы абонента в системе. Подчиненные сервера СРР выполняют те же функции в зоне своей ответственности. По запросу главного сервера подчиненные серверы высылают отчет о своей работе. Программные агенты СРР, встроенные в СЗИ абонентов, выполняют команды, поступающие от главного либо подчиненного сервера, высылают квитанции с результатом выполнения команды, формируют и отправляют главному серверу тревожные сообщения о сбоях своей работы.

Мониторинг и управление осуществляется посредством формирования и рассылки команд и сообщений в направлениях сервер ↔ агент и агент ↔ сервер. В СРР существуют три типа сообщений: команда управления, команда мониторинга, инициативное сообщение абонента.

В список команд управления входят следующие команды:

- установить ключ;
- уничтожить ключ;
- зарегистрировать абонента;
- блокировать работу абонента;
- разрешить работу абонента.

В список команд мониторинга входят следующие команды:

- проверить целостность программного обеспечения СЗИ абонента;
- проверить целостность ключевой информации абонентов;
- проверить правильность работы шифратора;
- выдать статистику объема обработанной (зашифрованной/расшифрованной) информации.

Команды формируются и рассылаются серве-

рами СРР в автоматическом режиме либо под управлением оператора. Команды имеют следующие идентификаторы: код команды, длина, приоритет, период повтора, время ожидания квитанции.

На команды, рассылаемые серверами СРР, агенты должны отправлять квитанции с результатами выполнения команд. На основе квитанций заполняются журналы безопасности и накапливается статистика о работе подсистемы защиты информации. В случае неполучения квитанции в заданный период ожидания сервер повторяет команду. Факт неполучения квитанции также заносится в журнал.

К инициативным сообщениям абонентов относятся сообщения о сбоях в работе средств защиты информации, нарушениях целостности ключевой информации или программного обеспечения СЗИ абонента, обнаружениях фактов несанкционированного доступа к радиостанции абонента. Сообщения отправляются серверу СРР, в зоне ответственности которого находится абонент. При получении сообщения о сбоях в ключевой информации сервер должен по каналам связи установить новые ключи. При получении остальных сообщений сервер должен блокировать работу данного абонента в системе связи и отправить команду "удалить ключевую информацию".

Ключевое обеспечение подсистемы защиты информации ГСС: ключевая структура ГСС должна позволять не только защищать каналы связи от несанкционированного прослушивания и вмешательства сторонних лиц, но и обеспечивать конфиденциальность связи двух абонентов или группы абонентов системы. При этом конфиденциальный канал связи должен предоставляться в произвольный момент времени.

Для обеспечения поставленных задач предлагается использовать следующую организацию ключевого обеспечения.

У каждого абонента системы есть свой инди-

видуальный ключ (ИК), абонентский ключ связи (АКС), циркулярный ключ связи (ЦКС).

На ретрансляторах космического сегмента присутствуют ИК, АКС ЦС, АКС всех ЗС, АКС всех абонентов системы, ЦКС.

На ЦС присутствуют ИК всех ретрансляторов, ИК всех ЗС, ИК всех АС, АКС всех ЗПС, АКС всех АС, а также циркулярный ключ.

На ЗС присутствуют собственный ИК, ИК всех подчиненных АС, собственный АКС, АКС всех подчиненных АС, циркулярный ключ.

Распределение ключей между элементами ГСС показано на рис. 3.

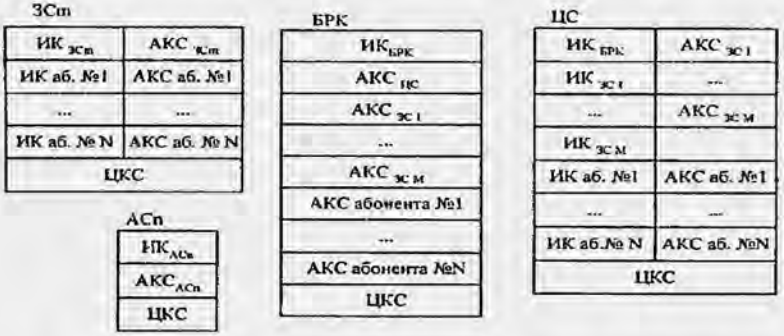


Рис. 3. Распределение ключей между элементами ГСС

ИК используется при зашифровании и имитозащите команд и сообщений, генерируемых СРР, а также всей информации передаваемой по каналу управления РТР и каналам управления ЗС; АСК — для зашифрования и имитозащиты информации, передаваемой по каналам связи глобальной и зональной сети; ЦКС — для зашифрования и имитозащиты информации, передаваемой по каналам связи и предназначенной для всех абонентов.

Принципы защиты каналов связи и каналов управления: информация передается по каналам связи и по каналам управления в формате паке-

тов, которые объединяются в суперкадр и передаются в выделенном временном интервале на заданной частоте и коде. Защита пакетов состоит из зашифрования информационного тела пакета и некоторых полей заголовка и просчета имитовставки от всех полей пакета.

Средство, организующее канал связи, осуществляет обработку и перешифрование информационных пакетов. Канал связи могут образовывать БРК, ЦС и ЗС. При этом радиолиния к организатору канала называется "Вверх", а от организатора канала — "Вниз".

Алгоритм обработки пакетов после организации канала состоит в следующем:

- абонент формирует пакет, зашифровывает его на своем АКС, формирует кадр и отправляет по радиолинии "Вверх";
- организатор принимает кадр, по идентификатору абонента выбирает АКС, расшифровывает пакеты, определяет абонента-получателя, находит АКС абонента-получателя и зашифровывает пакеты. Организатор формирует кадр и отправляет его по радиолинии "Вниз";
- абонент-получатель принимает кадр, расшифровывает пакеты, обрабатывает полученную информацию.

В СРР осуществляется дополнительная защита команд и инициативных сообщений на уровне СЗИ средств связи. Вся информация, генерируемая в рамках СРР и передаваемая по каналам связи, защищается на индивидуальных ключах абонентов.

Команды и сообщения инкапсулируются в информационные пакеты и отправляются по каналам связи. Если команда больше, чем длина информационного пакета, команда разрезается на части и передается по кускам. В СЗИ абонента команда или ее части расшифровываются, части склеиваются в целую команду. Команды и сообщения СРР передаются в общем потоке целевой информации. Распределение пакетов с

информацией СРР среди общего потока носит случайный характер, что затрудняет анализ и выявление управляющих команд и ключей. Принцип инкапсуляции команд в пакеты показан на рис. 4.

Рис. 4. Инкапсуляция команд в информационный пакет

Максимальная интенсивность рассылки команд от серверов СРР составляет 4 команды в сутки максимальной длины 350 бит. Максимальную длину имеет команда "установить ключ", в теле которой пересылается сам ключ (ключ — до 256 бит).

Длина информационного тела пакета составляет 100 бит; общая длина пакета — составляет 100 бит. Объем четырех команд возрастает до 750 бит.

Наложение помехоустойчивого кодирования (код Рида-Соломона со степенью кодирования 7/8) увеличивает объем передаваемой информации до 9600 бит [2]. При скорости передачи 2,4 кбит/с при отсутствии необходимости повторных передач пакетов время передачи четырех команд занимает 4 с для одного абонента. Необходимость в отправлении такого объема информации может возникнуть 1 раз в месяц.

Система радиомониторинга и радиоуправления средствами защиты информации является прозрачной для системы связи, не занимает канальный ресурс и не мешает работе абонентов.

В то же время создается механизм гибкого управления средствами защиты, оперативной смены ключей и сбора информации о состоянии подсистемы защиты информации. Ведение журналов и баз данных позволяет проводить анализ событий безопасности и выявлять факты сбоев и компрометаций. Большим преимуществом предложенной системы является наличие главного сервера СРР как пункта централизованного мониторинга, управления и сбора информации.

ЛИТЕРАТУРА

1. **Карташевский В. Г., Семенов С. Н., Фирстова Т. В.** Сети подвижной связи. — М.: Эко-Тренз, 2001. — 302 с.

2. **Скляр Б.** Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с англ. — М.: Изд. дом "Вильямс", 2003. — 1104 с.

Факсимильное издание.
Опубликовано в сборнике научных трудов межотраслевого научно-технического журнала «Оборонный комплекс — научно-техническому прогрессу России». — Москва, ФГУПВИМИ, 2005. — № 2. — С. 77–80.

Модулярная арифметика как криптографический примитив

Амербаев В. М., Дьячков В. Н.

В статье рассмотрены некоторые аспекты использования принципов модулярности (модульность и немодульность) в задачах информационной безопасности, базирующихся на симметричных шифр-системах.

Широкие возможности вычислительных средств выделили модульную арифметику или, в общем случае, арифметику кольца вычетов по модулю над кольцом главных идеалов [1] в особо важный класс управляемых примитивов криптографических преобразований. Это оказалось возможным благодаря

тому, что упомянутые алгебраические структуры допускают эффективную адаптацию их операций к регистровым операциям арифметических процессоров современных компьютеров.

То, что модульная арифметика лежит в основе многих важных криптопреобразований, является бесспорным фактом. Примером тому служат такие алгоритмы, как алгоритм RSA, алгоритм Эль-Гамаля, алгоритмы криптопреобразований над конечными полями.

Ниже пойдёт речь об использовании в криптопреобразованиях модулярной арифметики [2, 3], которая отличается от модульной тем, что здесь существенное значение приобретает понятие динамического диапазона. Дело в том, что в модулярной арифметике над кольцом целых чисел Z элементы кольца вычетов помимо кодовой интерпретации имеют и количественную трактовку, как целые числа. Поэтому здесь модульные вычисления над кодовыми словами в семантическом плане должны сопровождаться «мониторингом» возникновения возможных переполнений за основной диапазон, обычно называемый динамическим диапазоном, либо должны сопровождаться условиями, налагаемыми на операнды и операции, гарантирующими отсутствие подобных переполнений.

Несколько замечаний об используемых обозначениях и их смыслах.

- Символом $|x|_P$ обозначается вычет целого числа x по mod$P$.

По умолчанию этот же символ используется для обозначения наименьшего неотрицательного вычета.

- Z_P — кольцо вычетов по mod$P$:

$$\mathrm{Z}_P := \left\{ x \in \mathrm{Z} \,|\, |x|_P = x \right\}.$$

Связь кольцевых операций кольца Z_P с арифметическими операциями $+, \times$ над целыми числами выражается формулами

1) $\forall x, y \in \mathrm{Z}$,

$$|x + y|_P = \left| |x|_P + |y|_P \right|_P,$$

$$|x \times y|_P = \left| |x|_P \times |y|_P \right|_P;$$

2) мультипликативная инверсия — если $(M, P) = 1$, то вычет $x := |M^{-1}|_P$ есть решение уравнения $|x \cdot M|_P = 1$;

• $|x|_p^-$ — абсолютно наименьший вычет целого числа x по mod$P$:

$$\mathrm{Z}_P^- := \left\{ x \in \mathrm{Z} \,|\, -\frac{P}{2} \le x < \frac{P}{2} \right\}.$$

Связь абсолютно наименьшего вычета с наименьшим неотрицательным вычетом по mod$P$ выражается формулой

$$\forall x \in \mathrm{Z} : |x|_P^- = \left| x + \left\lfloor \frac{P}{2} \right\rfloor \right|_P - \left\lfloor \frac{P}{2} \right\rfloor.$$

Здесь $\lfloor a \rfloor$ — стандартное обозначение для наибольшего целого числа, не превосходящего $a \in R$:

$$\lfloor a \rfloor \le a < \lfloor a \rfloor + 1.$$

Модулярная арифметика в симметричных шифрах

1. Мультипликативный примитив

Секретные параметры:

$$P_1,\ P_2,\ \ldots,\ P_m,\ (P_i,\ P_{i+1}) = 1,$$

$$M_1,\ M_2,\ \ldots,\ M_m,\ (M_i, P_i) = 1.$$

Условие согласования:

$$P_1 < P_2 < \ldots < P_m.$$

Уравнение шифрации:

S — сообщение; $S \in \mathrm{Z}_{P_1}$:

$$\left\| |SM_1|_{P_1} M_2 \right|_{P_2} \ldots M_m \Big|_{P_m} = C.$$

Шифрация, описываемая последним уравнением, реализуется посредством m-раундов (итераций):

$$|SM_1|_{P_1} = x_1,$$

$$\left|x_1 M_2\right|_{P_2} = x_2,$$

...

$$\left|x_{m-2} M_{m-1}\right|_{P_{m-1}} = x_{m-1},$$

$$\left|x_{m-1} M_m\right|_{P_m} = C;$$

C — шифрограмма.

Процедура расшифрации (обоснование однозначности)

Так как $(M_m, P_m) = 1$, то уравнение последнего раунда разрешимо в Z_{P_m}:

$$\left|x_{m-1}\right|_{P_m} = \left|C M_m^{-1}\right|_{P_m}.$$

Так как согласно $(m-1)$-му раунду шифрации $x_{m-1} \in Z_{P_{m-1}}$ и поскольку $Z_{P_{m-1}} \subset Z_{P_m}$, то

$$\left|x_{m-1}\right|_{P_m} = x_{m-1}.$$

Следовательно, корректно по вычету $\left|x_{m-1}\right|_{P_m}$ восстанавливается уравнение шифрации $(m-1)$-го раунда:

$$\left|x_{m-2} M_{m-1}\right|_{P_{m-1}} = x_{m-1}.$$

Продолжая этот процесс возврата к исходному сообщению, на m-ом шаге получим:

$$S = \left|x_1 M_1^{-1}\right|_{P_1}.$$

В соответствии с двумя интерпретациями вычета процессы шифрации и расшифрации могут разворачиваться двумя путями.

Если модули $P_1, P_2, ..., P_m$ выбираются, скажем, из диапазона

$$2^{t-1} < P_i < 2^t,$$

где t — разрядность динамического диапазона компьютера, то вычеты по этим модулям удобно интерпретировать как числа, представленные позиционным кодом процессора; поэтому процессы шифрации и расшифрации осуществляются

в компьютерных командах над «компьютерными» числами: «выделить целую часть», «найти остаток», «умножить», «сложить» и т. п.

Так, организованную шифросистему будем называть мономодульной длины m. Для ускорения расшифрации, естественно, следует предвычислить константы $|M_1^{-1}|_{P_1}$, …, $|M_m^{-1}|_{P_m}$.

Разумеется, допустима организация прямого произведения n мономодульных схем шифрации фиксированной длины m и, вообще говоря, с различным ключевым материалом.

Мономодульные схемы хорошо укладываются в схемы поточных шифраторов с конвейерной структурой и управляемыми параметрами (M_i).

2. Модулярный примитив

Естественно, возникает модулярный вариант, если модули P_1, P_2, ..., P_m имеют вид

$$P_i = \prod_{j=1}^{r_i} p_j^{(i)},$$

где $p_1^{(i)}$, …, $p_{r_i}^{(i)}$ — попарно взаимно просты. В этом случае интерпретация вычетов для каждого i по $\mathrm{mod} P_i$ имеет только кодовую трактовку (модулярный код). Теперь, скажем, операция

$$x_i := \left| x_{i-1} M_i \right|_{P_i}$$

на i-м раунде шифрации реализуется следующим образом.

Так как вычет x_{i-1} представлен модулярным кодом по основаниям модуля P_{i-1}, то первым шагом необходимо перевести его в модулярный код по основаниям модуля P_i. Соответствующая операция в модулярной арифметике называется операцией расширения кодового представления с динамического диапазона $\mathrm{Z}_{P_{i-1}}$ на динамический диапазон Z_{P_i}. Известно, что эта операция равнозначна восстановлению величины числа. Вторым шагом выполняется модульное умножение результата операции расширения на M_i по основаниям модуля P_i.

Модулярная схема отличается существенно более глубоким перемешиванием на межраундовых шагах шифрации в связи с переходом от одних секретных модулей к другим.

Интерес также представляет аддитивный вариант рассматриваемых схем, где вместо операции модульного умножения на M_i на каждом i-м раунде используется операция модульного сложения.

Объединение этих подходов приводит к криптопримитиву с управляемой структурой алгоритма шифрации, которая управляется состоянием m-разрядного битового регистра: если на i-м раунде значение переменной $r_i = 1$, то используется мультипликативное преобразование, если же $r_i = 0$, то аддитивное.

3. Криптопреобразование горнеровского типа

Возможны и другие обобщения, например использование схемы криптопреобразований горнеровского типа. Пусть задан (для простоты изложения) полином 4-й степени:

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 \text{ над } Z_{P_1}.$$

Преобразование его по схеме Горнера имеет вид

$$a_0 + x\left(a_1 + x\left(a_2 + x(a_3 + a_4 x)\right)\right),$$

и оно порождает следующую итерационную процедуру вычислений значений полинома в точке x:

$$y_1 = a_3 + a_4 x,$$

$$y_2 = a_2 + y_1 x,$$

$$y_3 = a_1 + y_2 x,$$

$$y_4 = a_0 + y_3 x.$$

Криптопримитив горнеровского типа получается из последней итерационной схемы, если ее переписать в виде

$$y_1 = s_1 + a_4 k_1,$$

$$y_2 = s_2 + y_1 k_2,$$

$$y_3 = s_3 + y_2 k_3,$$

$$y_4 = s_4 + y_3 k_4,$$

где s_1, s_2, s_3, s_4 — компоненты кодового представления по $\mathrm{mod}\, P_1$ сообщения S; $k_1, k_2, k_3, k_4 \in Z_{P_1}$ — компоненты ключевого материала; a_4 — управляемый параметр.

Криптопреобразование горнеровского типа можно использовать на каждом раунде мультипликативного примитива, причем после каждого раунда целесообразно переставлять компоненты результата преобразования.

Подобные же конструкции синтезируются в кольце полиномов над конечными полями. Таким образом, возникает многообразие криптопримитивов.

Далее вопросы упираются в комплексную оптимизацию по таким параметрам, как стойкость, скорость, программная или аппаратная реализация криптопримитивов.

Стойкость здесь, как правило, обосновывается повышением качества рандомизированного управления как ключевым материалом, так и структурой алгоритмов шифрации на расширенном пространстве выборок. При этом под рандомизацией понимается управление выборкой посредством того или иного алгоритма детерминированного хаоса или псевдослучайного генератора.

Литература

1. Ленг С. Алгебра. — М.: Мир, 1968.
2. Акушский Н. Я., Юдицкий Д. И. Машинная арифметика в остаточных классах. — М.: Сов. радио, 1968.
3. Свобода А. Развитие вычислительной техники в Чехословакии. Система счисления остаточных классов (СОК) // Кибернетический сборник. — М.: Мир, 1964. — Т. 8.

Впервые опубликовано в трудах юбилейной научно-технической конференции «50 лет модулярной арифметике». — М.: МИЭТ, 2005. — С. 187–193.

Модулярный быстродействующий согласованный фильтр

Амербаев В. М., Стемпковский А. Л., Широ Г. Э.

Излагаются принципы построения, приводятся архитектура и оценки сложности аппаратной реализации цифрового согласованного фильтра, работающего в модулярной арифметике. Показано, что при аппаратных затратах, не превышающих таковые в фильтрах, построенных в обычной позиционной арифметике, предлагаемый фильтр обладает более высоким быстродействием — в два и более раза. Приводятся примеры.

General description, architecture, and estimations of apparatus complexity of the digital FIR Filter based on modular arithmetic are described. It is shown that the proposed filter is two — three times faster compare to one having same apparatus expenses but based on traditional position arithmetic. Examples are presented.

Постановка задачи

В радио- и звуколокации (radar, sonar) широкое применение находят согласованные фильтры как наиболее эффективное средство распознавания и временного сжатия сложных фазо- и частотно-модулированных сигналов. Рис. 1 иллюстрирует в качестве примера результат обработки линейно-частотно-модулированного (ЛЧМ) сигнала согласованным фильтром.

В соответствии с классической теорией цифровых линейных систем согласованный фильтр реализует формулу свертки:

$$\dot{sv}(n+z) = \sum_{k=1}^{K} \dot{s}(n-k) \cdot \dot{h}(k). \qquad (1)$$

Здесь $\dot{s}$, $\dot{h}$ — комплексные представления оцифрованных последовательностей сигнала и импульсной характеристики фильтра, n, k — соответственно номера отсчетов сигнала и импульсной характеристики, K — длина импульсной характеристики фильтра, $\dot{sv}$ — комплексное представление результата свертки, z — конвейерная задержка фильтра.

Для обеспечения условия согласования импульсной характеристики последняя выбирается зеркальной и комплексно-сопряженной относительно фазовой структуры сигнала:

$$\dot{h}(k) = \overline{\dot{s}}(-n).$$

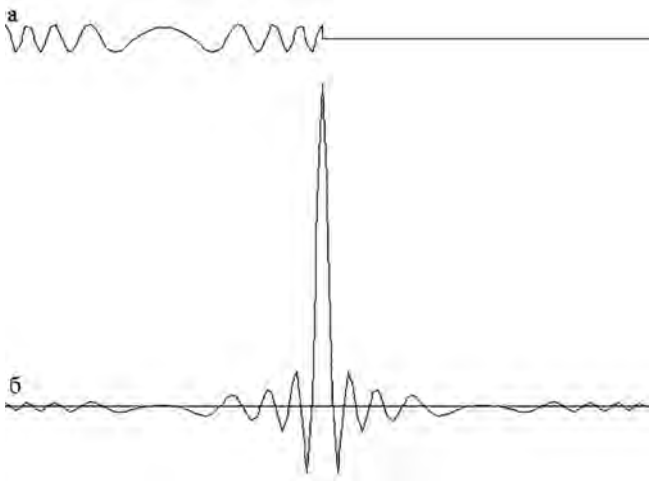


Рис. 1. Обработка ЛЧМ-сигнала цифровым согласованным фильтром: *а* — исходный сигнал; *б* — результат обработки

Аппаратная реализация цифрового согласованного фильтра
Непосредственная аппаратная реализация формулы (1), соответствующей цифровой согласованной фильтрации, выполняется по схеме рис. 2.

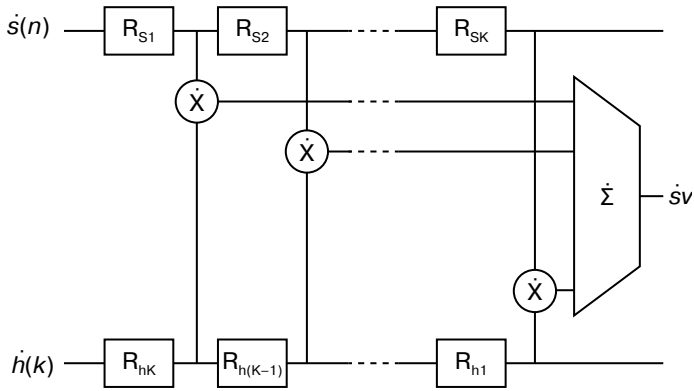


Рис. 2. Аппаратная реализация цифрового согласованного фильтра

Схема состоит из двух сдвиговых регистров *Rs* и *Rh* длиной *K* звеньев каждый, предназначенных для загрузки соответственно

комплексных отсчетов сигнала и опорной функции. Заметим, что нумерация звеньев в регистрах взаимно-обратная — в соответствии с требованиями зеркальной импульсной характеристики согласованного фильтра и в соответствии со знаком индекса k в формуле (1) при нумерации отсчетов сигнала $\dot{s}(n-k)$ импульсной характеристикой фильтра $\dot{h}(k)$.

Отсчеты сигнала и импульсной характеристики, хранящиеся в регистрах *Rs* и *Rh*, попарно перемножаются на комплексных умножителях, полученное произведение суммируется на комплексном пирамидальном сумматоре. Все упомянутые арифметические операции производятся в каждом (i-м) такте работы схемы, работающей с периодом T, равным периоду дискретизации сигнала.

Оценка аппаратной сложности цифрового согласованного фильтра, работающего в позиционной системе счисления

Основная вычислительная сложность схемы (рис. 2) приходится на комплексные умножители, число которых определяется длиной K фильтра, а разрядность — разрядностью операндов $r(\dot{s})$, $r(\dot{h})$. В качестве примера, имеющего практическое значение для реализации радиолокационных систем, здесь и далее будем рассматривать фильтр со следующими параметрами:

- длина K = 512 звеньев;
- разрядность $r(\dot{s}) = r(\dot{h}) = (12 + 12)$ разрядов, т. е. разрядность представления реальной (синфазной) и мнимой (квадратурной) составляющих равны по 12 разрядов;
- период дискретизации T = 10 нс.

Для простоты изложения числа $\dot{s}$ и $\dot{h}$ будем далее считать реальными: s, h.

Оценка аппаратной сложности $V^{П}$ схемы (рис. 2), построенной в позиционной системе счисления, может быть выражена формулой

$$V^{П} = O_V K r^2, \qquad (2).$$

где O_V — оценочный коэффициент, зависящий от применяемой элементной базы и, как будет показано ниже, от метода вычислений.

Применительно к обычно применяемой позиционной системе представления операндов r-разрядный матричный умножитель должен содержать r^2 полных трехвходовых сумматоров [1], каждый из которых может быть построен на 12 парах К-МОП-транзисторов.

Таким образом, оценку $V^{П}$ в парах К-МОП-транзисторов получаем равной $V^{П} = 12 \cdot K \cdot r^2$. Для рассматриваемого примера $V = 12 \cdot 512 \cdot 12^2 @ 900.000$ пар транзисторов.

Формула свёртки (1) может быть вычислена с помощью схемы, обладающей меньшей сложностью, чем по оценке (2), при переходе в частотную область и использовании процедур быстрого преобразования Фурье (БПФ). В ряде практических применений так и делают. Однако неизбежные при БПФ циклы вычислений, число которых по крайней мере $2 \log_2 K$, приводит к соответствующей конвейерной задержке длиной

$Dt = 2K \log_2 K$ тактов,

которая часто неприемлема.

Далее будем рассматривать вопрос аппаратной реализации только схемы (рис. 2), работающей во временной области, основное достоинство которой — возможность получения результата фильтрации с минимально возможной конвейерной задержкой, равной K тактов, т. е. равной длине импульсной характеристики фильтра.

Оценка быстродействия

Как было показано, основная аппаратная сложность реализации фильтра в виде вычислителя формулы свёртки (1) (рис. 2) определяется сложностью построения r×r-разрядных умножителей. Именно эти умножители определяют и быстродействие фильтра (минимальное значение T^{P}) периода дискретизации сигнала $\dot{s}(n)$, обрабатываемого фильтром в реальном масштабе времени.

Известно [1], что время T срабатывания матричного r×r-разрядного умножителя, построенного с использованием дерева Уоллеса и сумматора с предвычислением переносов имеет «оптимистичную» оценку быстродействия:

$$T^{P} = O \cdot 2\log_2(2r) \cdot t_1,$$

где t_1 — время предвычисления одного каскада переноса.

Для рассматриваемого примера разрядности r представления операндов r, равного 12, получим

$$T^P = O \cdot 2 \cdot \log_2 (2 \cdot 12) \cdot t_1 = O \cdot 10 \cdot t_1.$$

По-видимому, полученная оценка является теоретическим пределом повышения быстродействия умножителя, работающего в классической позиционной арифметике. Дальнейшее повышение быстродействия может быть получено за счет использования «модулярной» арифметики.

Принципы модулярной арифметики. Преимущества, недостатки

Воспользуемся следующими основными принципами представления чисел в «модулярной» арифметике и арифметических действий над ними [1].

Принцип 1: любое целое число a, находящееся в диапазоне 0, ..., N, может быть восстановлено по множеству вычетов — остатков от деления этого числа на множество модулей $\{m_1, m_2, ..., m_n\}$:

$$a \Leftrightarrow \{\alpha_1, \alpha_2, ..., \alpha_n\} = \{|a|_{m1}, |a|_{m2}, ..., |a|_{mn}\},$$

при этом модули m суть попарно взаимно простые числа и их произведение $M = m_1 m_2 ... m_n \le N$ перекрывает диапазон представления числа a.

Пример 1. Число a = 478, находящееся в диапазоне 0 ... 1309, может быть представлено в модулярном виде:

$$478 = \{|478|_7, |478|_{11}, |478|_{17}\} = \{2, 5, 2\}.$$

Здесь в качестве модулей выбраны попарно взаимно простые числа $\{m_1, m_2, m_3\} = \{7, 11, 17\}$, произведение которых $M = 7 \cdot 11 \cdot 17 = 1309$.

Для восстановления числа a по его модулярному представлению воспользуемся алгоритмом, основанным на китайской теореме об остатках [1].

Вычислим для выбранного набора модулей набор структурных чисел $\{k_1, k_2, k_3\}$:

$$k_1 = \left|\frac{M}{m_1}\right|_{m_1} = \left|\frac{1309}{7}\right|_7 = 5;$$

$$k_2 = \left|\frac{M}{m_2}\right|_{m_2} = \left|\frac{1309}{11}\right|_{11} = 9;$$

$$k_3 = \left|\frac{M}{m_3}\right|_{m_3} = \left|\frac{1309}{17}\right|_{17} = 9.$$

Для полученных структурных чисел вычислим обратные им:
$\{|k_1^{-1}|_{m1}, |k_2^{-1}|_{m2}, |k_3^{-1}|_{m3}\}$:

$$|k_1 k_1^{-1}|_{m1} = 1 \Rightarrow |5 \cdot 3|_7 = 1, \text{ следовательно, } k_1^{-1} = 3;$$

$$|k_2 k_2^{-1}|_{m2} = 1 \Rightarrow |9 \cdot 5|_{11} = 1, \text{ следовательно, } k_2^{-1} = 5;$$

$$|k_3 k_3^{-1}|_{m3} = 1 \Rightarrow |9 \cdot 2|_{17} = 1, \text{ следовательно, } k_3^{-1} = 2.$$

Теперь число a может быть восстановлено по формуле

$$a = \left|\alpha_1 k_1^{-1}\frac{M}{m_1} + \alpha_2 k_2^{-1}\frac{M}{m_2} + \alpha_3 k_3^{-1}\frac{M}{m_3}\right|_M;$$

$$a = \left|2 \cdot 3\frac{1309}{7} + 5 \cdot 5\frac{1309}{11} + 2 \cdot 2\frac{1309}{17}\right|_{1309} = 478.$$

Пример 2. Число b = −478, находящееся в диапазоне $-\frac{1309}{2} \ldots + \frac{1309}{2}$, при сохранении предыдущего набора модулей {7, 11, 17} может быть представлено в модулярном виде следующим образом.

Для отрицательного числа вычислим его дополнение до M:

$$\bar{b} = M - 478 = 1309 - 478 = 831.$$

Теперь представим $\bar{b}$ в модулярном виде:

$$b \Rightarrow \bar{b} \Leftrightarrow \{|813|_7; |831|_{11}; |831|_{17}\} = \{5, 6, 15\}.$$

Принцип 2: сумма (произведение) по модулю m двух чисел a, b равна сумме (произведению) по этому модулю вычетов этих чисел:

$$|a + b|_m = |a|_m (+_m) |b|_m,$$

$$|a \cdot b|_m = |a|_m (*_m) |b|_m.$$

Здесь $(+_m)$, $(*_m)$ — операции сложения и умножения по модулю m, алгоритмы которых аналогичны алгоритмам представления чисел по модулю m:

$$a (+_m) b = |a + b|_m, \qquad a (*_m) b = |a \cdot b|_m.$$

Пример 3. $|46 + 19|_7 = |46|_7 (+_7) |19|_7$

$$2 = |4 + 5|_7$$

$$2 = 2.$$

Пример 4. $|46 \cdot 19|_7 = |46|_7 (*_7) |19|_7$

$$6 = |4 \cdot 5|_7$$

$$6 = 6.$$

Рассмотренные свойства модулярной арифметики позволяют сделать важный для практики вывод: операции сложения и умножения (положительных и отрицательных чисел) могут выполняться не с исходными числами, а с вычетами, для каждого модуля отдельно.

Поскольку величины модулей, а следовательно, и вычетов существенно меньше, чем исходные числа, операции сложения и умножения могут выполняться на малоразрядных быстродействующих сумматорах и умножителях.

Данное преимущество приходится «оплачивать» процедурами преобразования операндов из позиционного представления в модулярное и обратно. Применительно к рассматриваемой задаче построения цифрового согласованного фильтра эта «плата» оказывается приемлемой: прямое и обратное преобразования здесь достаточно выполнять на входе и на выходе длинного вычислительного конвейера. При этом основной объем вычислений выполняется в модулярной арифметике.

Умножение в системе «дискретных логарифмов»

При построении умножителей, работающих в модулярной арифметике, можно воспользоваться индексным или «дискретно-логарифмическим» представлением операндов и заменить операцию модулярного умножения операцией модулярного сложения индексов или дискретных логарифмов [1].

Дискретно-логарифмическое представление модулярного числа $\log_{\omega}^{D}|a|_{m}$ основывается на понятии первообразного «корня по простому модулю m». Таким корнем $\omega(m)$ является целое число, возведение которого в степень 1, 2, ..., $(m-1)$ дает неповторяющиеся вычеты по модулю m.

Например, для $m = 7$ первообразным корнем является $\omega(7) = 3$.

Действительно:

$$|3^{1}|_{7} = |3|_{7} = 3,$$
$$|3^{2}|_{7} = |9|_{7} = 2,$$
$$|3^{3}|_{7} = |27|_{7} = 6,$$
$$|3^{4}|_{7} = |81|_{7} = 4,$$
$$|3^{5}|_{7} = |243|_{7} = 5,$$
$$|3^{6}|_{7} = |729|_{7} = 1.$$

Таким образом, получаем таблицу дискретных логарифмов (табл. 1).

Таблица 1. Дискретные логарифмы для $m = 7$

$\lvert a\rvert_{7}$	$\log_{3}^{D}\lvert a\rvert_{7}$
0	$-\infty$
1	6
2	2
3	1
4	4
5	5
6	3

Строка $0 \Leftrightarrow -\infty$ здесь введена искусственно, однако обработка нулевых вычетов и, соответственно, значений $\log^{D} = (-\infty)$ реализуема. См. пример 6.

Если столбцы в таблице 1 поменять местами и рассортировать строки по первому столбцу, получим таблицу антилогарифмов (табл. 2).

Таблица 2. Дискретные антилогарифмы для $m = 7$

$\log_3^D \lvert a \rvert_7$	$\overline{\log}_3^D \lvert a \rvert_7 = \lvert a \rvert_7$
$-\infty$	0
1	3
2	2
3	6
4	4
5	5
6	1

Теперь процедуру умножения вычетов можно представить следующим образом:

$$\lvert a \rvert_m (*_m) \lvert b \rvert_m = \overline{\log}_{\omega}^{D} \left[\log_{\omega}^{D}(a)(*_{m-1}) \log_{\omega}^{D}(b) \right].$$

Рассмотренный выше пример 4 можно решить следующим образом.

Пример 5.

$$6 = 4(*_7)5 = \overline{\log}_3^D \left[\log_3^D(4)(*_6) \log_3^D(5) \right] = \overline{\log}_3^D \left[4(+_6)5 \right] = \overline{\log}_3^D [3] = 6.$$

При вычислениях мы воспользовались таблицами 1, 2 дискретных логарифмов и антилогарифмов.

Следующий пример иллюстрирует применимость процедуры логарифмирования к нулевым операндам.

Пример 6.

$$\lvert 46 \cdot 0 \rvert_7 = 0,$$

$$0 = 4\ (*7)\ 0 = \overline{\log}_3^D \left[\log_3^D(4)(*_6) \log_3^D(0) \right] = \overline{\log}_3^D \left[4(+_6) - \infty \right] = 0.$$

При этом применимо следующее правило суммирования дискретных логарифмов при условии, что один из них равен — ∞:

$$x + (-\infty) = -\infty,$$

$$(-\infty) + x = -\infty,$$

$$(-\infty) + (-\infty) = -\infty.$$

Таким образом, операция умножения выполнена с помощью более экономной операции модулярного сложения, причём без увеличения разрядности операндов. «Платой» за полученную экономию являются операции логарифмирования и антилогарифмирования, выполнение которых требует соответствующих таблиц.

Пример 7. Решение задачи свёртки в модулярной дискретно-логарифмированной арифметике.

Пусть в цифровом согласованном фильтре с длиной импульсной характеристики K = 4 в некоторый *n*-й момент времени, т. е. в некотором n-ом такте, операнды приняли значения, соответствующие рис. 3. К окончанию этого такта на выходе фильтра должно быть получено число 71 — результат свёртки в данном такте.

Пусть результаты свёртки на любом такте не выходят за пределы $-\frac{1309}{2}...+\frac{1309}{2}$.

В качестве множества модулей выберем такие, произведение M которых не менее 1309:

$$1309 \le M = \{m_1 \cdot m_2 \cdot m_3\} = \{7,\ 11,\ 17\}.$$

Представим исходные операнды в модулярном виде, а затем — в дискретно-логарифмированном виде (табл. 3). При этом отрицательные числа взяты в виде дополнений до M, например:

$$-13 \Rightarrow 1309 - 13 = 1296,$$

$$|-13|_7 = |1296|_7 = 1.$$

Попарное умножение или попарное сложение дискретных логарифмов и затем вычисление антилогарифмов дают результаты, представленные в табл. 8.

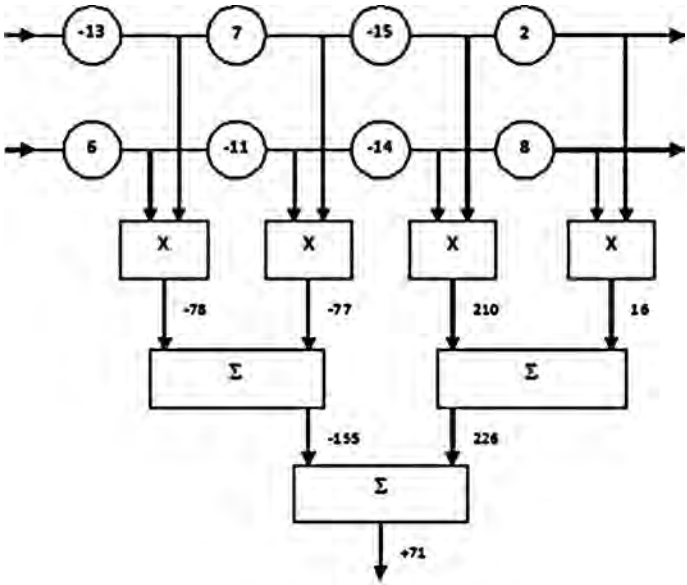


Рис. 3. Пример вычисления свёртки для произвольного (n-го) такта работы фильтра

Таблица 3. Преобразование операндов для примера 7: позиционная система → модулярное представление → дискретно-логарифмическое представление

Операнды	$\|x\|_{17}$	$\|x\|_{17}$	$\|x\|_{17}$	$\log_3^D \|x\|_7$	$\log_2^D \|x\|_{11}$	$\log_3^D \|x\|_{17}$
−13	1	9	4	6	6	12
6	6	6	6	3	9	15
7	0	7	7	−∞	7	11
−11	3	0	6	1	−∞	15
−15	6	7	2	3	7	14
−14	0	8	3	−∞	3	1
2	2	2	2	2	1	14
8	1	8	8	6	3	10

Кроме таблиц 1, 2 логарифмов и антилогарифмов для $m = 7$ потребуются аналогичные табл. 4, 5, 6, 7 для $m = 11$, $m = 17$. Первообразные корни здесь $\omega(11) = 2$, $\omega(17) = 3$.

Таблица 4. Дискретные логарифмы для $m = 11$

$\lvert a\rvert_{11}$	$\log_2^D \lvert a\rvert_{11}$
0	$-\infty$
1	10
2	1
3	8
4	2
5	4
6	9
7	7
8	3
9	6
10	5

Таблица 5. Дискретные антилогарифмы для $m = 11$

$\log_2^D \lvert a\rvert_{11}$	$\overline{\log_2}^D \lvert a\rvert_{11} = \lvert a\rvert_{11}$
$-\infty$	0
1	2
2	4
3	8
4	5
5	10
6	9
7	7
8	3
9	6
10	1

Таблица 6. Дискретные логарифмы для $m = 17$

$\lvert a\rvert_{17}$	$\log_3^D \lvert a\rvert_{17}$
0	$-\infty$
1	16
2	14
3	1
4	12
5	5
6	15
7	11
8	10
9	2
10	3
11	7
12	13
13	4
14	9
15	6
16	8

Таблица 7. Дискретные антилогарифмы для $m = 17$

$\log_3^D \lvert a\rvert_{17}$	$\overline{\log_3}^D \lvert a\rvert_{17} = \lvert a\rvert_{17}$
$-\infty$	0
1	3
2	9
3	10
4	13
5	5
6	15
7	11
8	16
9	14
10	8
11	7
12	4
13	12
14	2
15	6
16	1

Таблица 8. Результаты попарных перемножений операндов для примера 5 в дискретно-логарифмическом виде

$a \cdot b$	$\log_3^D\left[\lvert a\rvert_7(*_7)\lvert b\rvert_7\right] =$ $\log_3^D\lvert a\rvert_7(+_6)\log_3^D\lvert b\rvert_7$	$\log_2^D\left[\lvert a\rvert_{11}(*_{11})\lvert b\rvert_{11}\right] =$ $\log_2^D\lvert a\rvert_{11}(+_{10})\log_2^D\lvert b\rvert_{11}$	$\log_3^D\left[\lvert a\rvert_{17}(*_{17})\lvert b\rvert_{17}\right] =$ $\log_3^D\lvert a\rvert_{17}(+_{16})\log_3^D\lvert b\rvert_{17}$
$(-13)\cdot 6$	$6(+_6)3 = 3$	$6(+_{10})9 = 3$	$12(+_{16})15 = 11$
$7\cdot(-11)$	$(-\infty)\ (+_6)3 = (-\infty)$	$7(+_{10})(-\infty) = (-\infty)$	$11(+_{16})15 = 10$
$(-15)\cdot(-14)$	$3(+_6)\ (-\infty) = (-\infty)$	$7(+_{10})3 = 10$	$14(+_{16})1 = 15$
$2\cdot 8$	$2(+_6)6 = 2$	$1(+_{10})3 = 4$	$14(+_{16})10 = 8$

Воспользовавшись табл. 2, 5, 7 антилогарифмов и просуммировав результаты попарного перемножения в модулярном виде, получим результат свертки в модулярном виде (табл. 9).

Таблица 9. Окончательный результат для примера 5

$a \cdot b$	$\lvert a\rvert_7(*_7)\lvert b\rvert_7$	$\lvert a\rvert_{11}(*_{11})\lvert b\rvert_{11}$	$\lvert a\rvert_{17}(*_{17})\lvert b\rvert_{17}$
$(-13)\cdot 6$	6	10	7
$7\cdot(-11)$	0	0	8
$(-15)\cdot(-14)$	0	1	6
$2\cdot 8$	2	5	16
$\Sigma = 71$	$\lvert\Sigma_7\rvert = 1$	$\lvert\Sigma_{11}\rvert = 5$	$\lvert\Sigma_{17}\rvert = 3$

Модулярное представление числа 71:

$$71 \Rightarrow \{\lvert 71\rvert_7, \lvert 71\rvert_{11}, \lvert 71\rvert_{17}\} = \{1, 5, 3\}.$$

Функциональная схема фильтра, работающего в «модулярной арифметике»

Модулярный принцип представления данных позволяет распараллелить вычислительный процесс и, соответственно, схему фильтра на m параллельных функционально-идентичных каналов — рис. 4.

Рассмотрим функциональную схему одного канала модулярного вычислителя, обрабатывающего данные по одному (i-му) модулю m_i — рис. 5. Для простоты изложения отсчёты

сигнала s(n) и импульсной характеристики h(k) принимаем не комплексными, а реальными.

Подобно схеме фильтра, работающего в позиционной системе (рис. 2), схема рис. 5 содержит два K-звенных сдвиговых регистра для хранения и сдвига отсчётов сигнала и опорной функции. Отличие здесь в представлении чисел s(n), h(k) — позиционная система, с одной стороны, $\log^D|s|_{mi}$,

Рис. 4. Функциональная схема фильтра

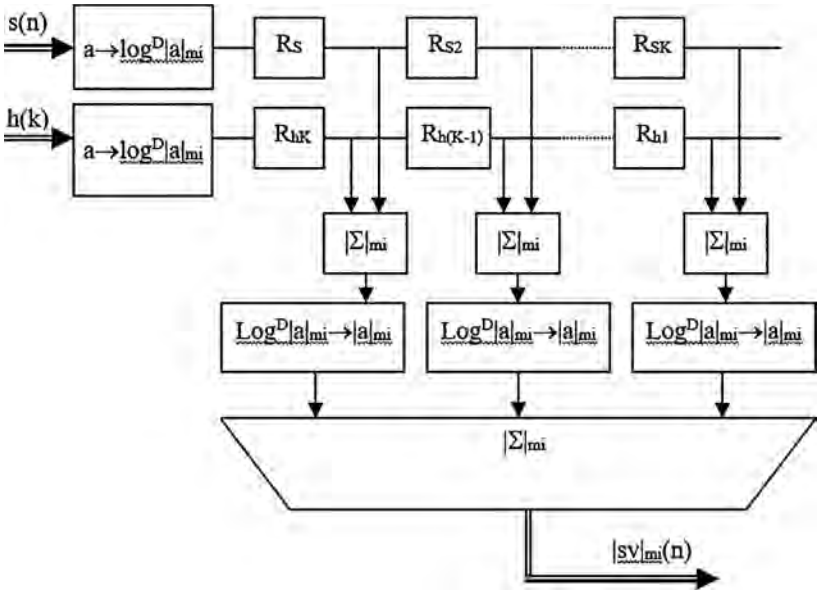


Рис. 5. Функциональная схема модулярного вычислителя

$\log^D|h|_{mi}$ — модулярная дискретно-логарифмическая система — с другой. Для получения чисел в модулярной дискретно-логарифмической форме на входе сдвиговых регистров стоят функциональные преобразователи а ® $\log^D|a|_{mi}$.

Роль умножителей схемы рис. 2 в схеме рис. 5 выполняют модулярные сумматоры $|S|_{mi-1}$, и это главное преимущество. Для выполнения последующего суммирования полученных результатов последние должны быть преобразованы из дискретно-логарифмической в модулярную форму $\log^D|a|_{mi}$ ® $|a|_{mi}$. Эти антилогарифмические преобразователи — «плата» за отсутствие в схеме рис. 5 умножителей. Число преобразователей K равно числу звеньев фильтра. Как будет показано далее, именно они в основном определяют уровень интеграции микросхемы, реализующей функциональную схему рис. 5.

Пирамидальный сумматор $|S|_{mi}$ строится из сумматоров по модулю m_i, аналогичных обыкновенным «позиционным» сумматорам. Выходной преобразователь модулярных кодов в позиционные (рис. 4) реализует алгоритм, основанный на китайской теореме об остатках. Пример работы этого алгоритма был рассмотрен выше.

Оценка аппаратной сложности цифрового согласованного фильтра, работающего в «модулярной арифметике»

Оценку аппаратной сложности схемы рис. 4, 5 вычислим применительно к рассмотренному выше примеру 12-разрядного фильтра с длиной импульсной характеристики K = 512. Набор модулей должен быть выбран таким, чтобы их произведение M перекрывало диапазон представления результата свёртки sv:

$$M \geq 2^{12} \cdot 2^{12} \cdot 512 = 2^{33}.$$

Данному условию удовлетворяет, например, следующий набор простых чисел:

$$2^{33} \leq M = m_1 \cdot m_2 \cdot \ldots \cdot m_n = 3, 5, 7, 13, 17, 19, 23, 29, 31.$$

Для кодировки данного набора потребуется 37 разрядов:

$$\log_2 m_1 + \log_2 m_2 + \ldots + \log_2 m_n = 2 + 3 + 3 + 4 + 5 + 5 + 5 + 5 + 5 = 37.$$

Ограничимся, как ранее, оценкой (2) аппаратной сложности умножителей. В схеме рис. 5 основная сложность умножителей приходится на таблицу дискретных логарифмов. При реализации этих таблиц в виде ПЗУ суммарная емкость ПЗУ для одного умножителя будет равна

$$V_{пзу} = (m_1 \cdot \log_2 m_1 + m_2 \cdot \log_2 m_2 + ... + m_n \cdot \log_2 m_n) \text{ бит} =$$

$$= (3 \cdot 2 + 5 \cdot 3 + 7 \cdot 3 + 13 \cdot 4 + 17 \cdot 5 + 19 \cdot 5 + 23 \cdot 5 + 29 \cdot 5 + 31 \cdot 5) \text{бит} = 689 \text{ бит.}$$

Таблицы антилогарифмов обладают свойством симметрии, обусловленной коммутативностью умножения и знаковой симметрией абсолютно наименьших вычетов, с учётом которой

$$V_{пзу} = 689 \cdot 0{,}25 \approx 173 \text{ бит.}$$

При реализации ПЗУ на К-МОП-транзисторах при условии кодировки одного бита одной парой К-МОП-транзисторов получим $V_{пзу} = 173$ пар транзисторов.

Для рассматриваемой в примере длины импульсной характеристики $K = 512$ получим оценку аппаратной сложности фильтра в целом:

$$V^{М} = 512 \cdot V_{ПЗУ} = 512 \cdot 173 = 88.000 \text{ пар транзисторов.}$$

Данная оценка значительно лучше полученной ранее для фильтра, работающего в позиционной арифметике: $V^{П} \approx 900.000$ пар транзисторов. Соотношение $\frac{V^{П}}{V^{М}} \approx 9$ в пользу «модулярной арифметики».

Преимущества «модулярного» варианта сохраняются и при уточнении оценок. В случае «позиционного» варианта оценку необходимо увеличить с учетом того, что в схеме должны быть применены не простые матричные умножители, а быстродействующие [1]. С другой стороны, для «модулярного» варианта необходимо учесть увеличение по сравнению с «позиционным» разрядности входных регистров (для рассматриваемого примера — в три раза).

Оценка быстродействия цифрового согласованного фильтра, работающего в «модулярной» арифметике

Быстродействие T^M схемы рис. 5, работающей в «модулярной» арифметике, определяется быстродействием сумматоров, работающих по максимальному модулю m_n. В рассматриваемом примере $m_n = 31$. Разрядность соответствующего сумматора равна 5. Следовательно,

$$T^M = O \cdot 5 \cdot t_{пер},$$

где $t_{пер}$ — время переноса сумматора.

Данная оценка лучше полученной ранее для фильтра, работающего в позиционной арифметике: $T^P = O \cdot 10 \cdot t_{пер}$. Соотношение $\frac{T^P}{T^M} = 2$ в пользу «модулярной» арифметики.

Преимущества «модулярного» варианта сохраняются и даже увеличиваются при уточнении оценки T^P. Для быстродействующего умножителя, применяемого в схеме рис. 2, время предвычисления переноса в полтора—два раза больше времени вычисления переноса в трехвходовых сумматорах, на которых строится схема рис. 5.

Выводы

1. Эффективным методом построения быстродействующих цифровых согласованных фильтров, работающих в реальном времени, является использование «модулярной арифметики», при которой оцифрованные исходные данные на входе фильтра преобразуются из позиционной системы счисления в модулярную систему, все промежуточные вычисления производятся в модулярной системе, затем на выходе фильтра результирующие данные преобразуются в позиционную систему.

2. Аппаратная сложность фильтра, рассмотренного в качестве примера, с длиной импульсной характеристики $K = 512$ и разрядностью операндов, равной 12, построенного по «модулярному» принципу, оказывается существенно меньшей, чем для аналогичного фильтра, работающего в обычной позиционной арифметике. При возрастании разрядности операндов преимущества «модулярного» принципа увеличиваются.

3. Главным преимуществом построения фильтров по модулярному принципу является повышение быстродействия, что для устройств, работающих в реальном времени, является решающим требованием. Максимальная величина задержки в таких фильтрах определяется временем срабатывания малоразрядных сумматоров (в примере — пять разрядов). По сравнению с аналогичным фильтром, работающим в позиционной системе, достигается выигрыш в быстродействии в два и более раза.

4. Так как на промежуточных этапах фильтрации по модулярному принципу не производится округление (как это имеет место в позиционном варианте), то результат фильтрации по модулярному принципу имеет максимально достижимую точность для данного типа фильтрации.

Литература

1. Т. Кормен, Ч. Лейзерсон, Р. Ривест. Алгоритмы. Построение и анализ / Пер. с англ. А. Шеня. — МЦНМО. — М., 1999. — 960 с., 263 ил.

Впервые опубликовано в трудах юбилейной научно-технической конференции «50 лет модулярной арифметике». — М.: МИЭТ, 2005. — С. 250–267.

Зеленоград — город больших планов, надежд и дел на благо Родины

Амербаев В. М.

Впервые о проекте строительства города-спутника (города-спальни) Москвы (будущего Зеленограда) я узнал в конце пятидесятых, когда завершал как аспирант в Математическом институте им. В. А. Стеклова работу над кандидатской диссертацией. Тогда я не мог даже помыслить, что Зеленоград станет для меня городом становления моей зрелой творческой и духовной жизни, родиной всех моих внуков и, по существу, моей второй родимой землёй: здесь твёрдыми ножками уже топает мой годовалый правнук Дима. Имя «Дмитрий» дорого всем москвичам как имя великого князя — Дмитрия Донского.

Мне дорого оно и потому, что в годы аспирантуры, вдали от моей молодой семьи, в те дни, когда требовались душевная поддержка и отдохновение, я всё это находил в тенистом саду на святой земле Донского монастыря (благо он находился на пути между «Ленинкой» и общежитием академии наук). Здесь я часто в одиночестве проводил своё свободное время, размышляя не только о научных проблемах. Это были благостные моменты: здесь, к своему удивлению, я получал заряд бодрости, вдохновения и очищения от всякого рода тягостей. Случилось так, что всю жизнь я был в окружении деревьев, зелень для меня — святой цвет. Алма-Ата, где я провёл молодость, первую треть жизни, — прекрасный город в предгорьях Тянь-Шаня, утопающий в зелени. Своей удивительной зеленью манил к себе и Донской монастырь. Но когда я впервые оказался в Зеленограде, врезанном в лес, он навеки покорил меня. Зеленоград строился людьми, наделёнными великим чувством друидов — любовью к деревьям! Я видел, как строители обрезали дом, не достраивая его вторую половину, если он натыкался на кромку даже небольшой рощицы, хотя вокруг шумел многовековой лес. Это бережное отношение к зелёному другу потрясло меня! И я понял, что в Зеленограде живут замечательные люди и что не зря они свой город назвали ласковым словом — Зеленоград. Я счастлив, что судьба моя привела меня сюда, где у деревни Крюково стояли насмерть вместе с героическими защитниками Москвы бойцы Панфиловской дивизии, которая формировалась в Алма-Ате. И надо было так случиться, что я пацаном босиком в конце лета сорок первого года провожал с мамой эту дивизию, которая маршем по проспекту Сталина двигалась к вокзалу «Алма-Ата-2», оттуда отправившись на фронт. Отец мой к тому времени был на Ленинградском фронте, а его брат лежал в госпитале в Химках, где вскоре скончался от ран. Эта цепочка незримых для меня связей далёкой Алма-Аты с Зеленоградом продолжилась, когда я на приёме у начальника отдела кадров НИИФП встретился с Петром Васильевичем Логвиненко — комиссаром одного из полков панфиловской дивизии, уроженцем наших краёв, а директором института оказался молодой доктор физико-математических

наук, профессор Виталий Иванович Стафеев, который закончил двумя годами раньше меня Казахский государственный университет им. С. М. Кирова, наш родной физико-математический факультет. В то время я ничуть не удивлялся этой незримой цепочке связи. Воспринимал её как данность, так как был абсолютно убеждён, что мы все — люди одной большой и прекрасной семьи, повязаны одной единой связью — любовью к нашей Родине, долгом служить и быть полезным ей. Везде я встречал дружелюбие и внимательность, что оставляло меня таким, каким я был в «родных пенатах».

Как произошло, что в конце шестьдесят пятого я оказался в Зеленограде? К тому времени я заведовал лабораторией машинной и вычислительной математики при президиуме Академии наук Казахстана. Моя семья получила удобную двухкомнатную квартиру в новом доме, и у меня уже была вторая дочь, которой исполнилось полтора года. В мае 1965 года к нам на конференцию приехали из Москвы И. Я. Акушский и Д. И. Юдицкий, они рассказали о новом научном направлении в области вычислительной техники и поставили ряд задач. Хотя в то время я увлекался другим научным направлением, но в одной из поставленных задач увидел родство с методом решения ранее рассмотренных мною задач. Всю ночь я работал над возникшей идеей и утром следующего дня рассказал дорогим гостям о своих наблюдениях. Во второй половине дня ко мне подошёл Д. И. Юдицкий и предложил работу в Зеленограде. Я понимал, что от добра добра не ищут, но меня очень заинтересовало новое (вообще говоря, необычное) направление параллельных вычислений.

Моя жена Эмилия Нестеровна, учительница географии, всегда поддерживала мои научные пристрастия. И поэтому на мой вопрос: «Как быть» — ответила: «Поступай как считаешь нужным», хотя отъезд из Алма-Аты, где моя семья уже получила некоторый положительный статус и рядом были любимые родители и много родственников, казался на тот момент диковатым. Я объявил руководству о приглашении работать в Москве (тогда работа в Москве имела высочайший престиж), и меня отпустили с добром, напутствуя не терять связи с родной академией.

Первые жилые микрорайоны и промышленные зоны Зеленограда

Так я оказался в Зеленограде и был зачислен в НИИФП. Был молод не только сам город, но и, по существу, абсолютное большинство его жителей. Ориентация города к тому времени сменилась на новую — создать «отечественную Кремниевую долину». На всех участках труда люди были полны энтузиазма. У всех в глазах светился огонёк служения Родине, Науке. Это чувствовалось везде: на стройках, в организации новых научных институтов, в сфере обслуживания, где было абсолютное удовлетворение бытовых условий: обилие детских садов и школ, общественных столовых, мастерских бытового обслуживания, и, главное, в становлении высшего учебного заведения мирового стандарта — МИЭТа. Никакого чванства, максимум деловитости, общий порыв. Я вспоминаю ранние годы становления Научно-исследовательского института физических проблем. Научные семинары, поиск истины в спорах, сопоставлениях, оценках. Я не жалел, что покинул обжитые места — начиналась новая жизнь: я оказался в молодом творческом коллективе, перед которым (как, впрочем, и перед коллективами других институтов) были поставлены интереснейшие животрепещущие и важные для государства и народа задачи. Все трудились с высокой отдачей. Каждый чувствовал свою причастность к проблеме большой государственной важности. Это был большой порыв

молодого города, призванного служить своему народу. Город и сейчас продолжает развиваться, обрастать новостройками, новыми возможностями и осмылением своей предназначенности.

Фрагмент Зеленограда сегодня
(https://www.netall.ru/gnn/130/580/222166.html)

Пусть всегда Зеленоград остаётся зелёным раем, освещённым солнцем мира, наделённым молодостью и высокими трудовыми достижениями. Здесь, как и всюду в активных зонах Родины, рождается новая Россия.

Опубликовано в кн.
«Корни и крона Зеленограда». —
М.: Алфея и К, 2007. — С. 22–24.

Модулярная логарифметика — новые возможности для проектирования модулярных вычислителей и преобразователей (краткий обзор)

Стемпковский А. Л., Амербаев В. М., Корнилов А. И.

Аннотация **— В сообщении привлекается внимание разработчиков к модулярной логарифметике. Указанной арифметике уделяется большое внимание начиная с 90-х годов прошлого столетия. В сообщении отмечаются конструктивные особенности модулярной логарифметики, которые требуют разработки новых более прогрессивных методов проектирования модулярной арифметики.**

Ключевые слова **— модулярная арифметика, логарифметика поля GF(p), дискретный логарифм, логарифм Якоби.**

I. Введение

Общеизвестно, что десятичная система счисления – величайшее достижение в истории человеческой мысли, существенно упростила счет и вычисления, что послужило революционным толчком для технического прогресса, а после изобретения бесконечных десятичных дробей она приобрела статус универсальной системы счисления архимедовой математики. Двоичная система счисления составила основу современного технического прогресса не только в области проектирования и производства вычислительных средств на современной элементной базе микро- и наноэлектроники, но и в сфере современных информационных технологий. Вместе с тем внутренние проблемы развития технического прогресса стимулируют как рост вычислительной потребности, так и совершенствование вычислений при решении тех или иных специальных задач. Так, после того, как десятичная система счисления была привнесена в 16 веке

в Европу, бурное развитие получили астрономия и мореплавание, которые в 17 веке стимулировали рост вычислительной потребности. В результате возник логарифм, как средство, облегчающее трудоемкость операций умножения и деления чисел в десятичной системе счисления. Бурный рост вычислительной потребности во второй половине XX века поставил новые острые проблемы в области вычислительных технологий и технологий проектирования. Это:

- ускорение вычислений (методы распараллеливания как на уровне алгоритмов и программ, так и на уровне машинных кодов);
- отказоустойчивость арифметических вычислений (разработка систем арифметичной самокоррекции, т.е. систем обнаружения и исправления ошибок в режиме компьютинга – непрерывного вычислительного процесса);
- разработка реконфигурируемых вычислительных структур;
- разработка систем автономного компьютинга, т.е. вычислительных систем длительного автономного существования;
- разработка потоковых вычислений;
- разработка арифметико-логических средств повышения «процента выхода годных кристаллов» на этапе производства изделий на кристалле;
- криптографическая стойкость специализированных вычислительных систем открытого доступа и т.п.

Все эти проблемы возникают при решении задач проектирования широкого спектра цифровых устройств специального назначения. Однако межразрядные связи позиционной арифметики делают практически невозможным эффективное решение их на уровне машинных кодов. Что же касается надежности вычислений, то здесь остается, по существу, единственный путь – кратное резервирование аппаратуры.

В связи с этим актуальна задача – разработать такую систему компьютерного счета, в рамках которой

открывались бы пути практически приемлемых решений перечисленных выше проблем. Одним из претендентов на такого рода систему компьютерного счета является модулярная арифметика, возникшая более полувека назад. Ей присущи такие свойства, как параллелизм и арифметичная самокоррекция машинных кодов. Однако, такие важные операции машинной арифметики, как деление, формирование признака переполнения, округление, перевод из одной системы счисления в другую, а также алгоритмы декодирования системы самокоррекции являются, существенно, последовательно - параллельными. Перечисленные операции принято называть немодульными. Следовательно, класс вычислительных задач, где могут быть достигнуты успехи средствами модулярной арифметики, оконтуривается двумя требованиями к вычислительным процессам: низким процентным составом немодульных операций и/или допускающими сокращение немодульных операций посредством технически (экономически) допустимого увеличения вычислительного диапазона цифрового устройства.

Таким образом, модулярная система счисления не может претендовать на статус универсальной системы счисления. Однако, ее использование при решении многокритериальных математических и технических задач проектирования вычислительных средств, как показывает опыт большого числа разработчиков [1], может содействовать повышению эффективности принятия проектных решений. Популярность модулярной арифметики в среде разработчиков специальных вычислительных средств велика – об этом говорит библиография работ, приведенная в сборнике научных трудов юбилейной международной научно-технической конференции «50 лет модулярной арифметике», проведенной в 2005 году в рамках V международной научно-технической конференции «Электроника и информатика 2005», МИЭТ, Москва [2]. Библиография содержит более 1500 работ. Спрос на

модулярную арифметику также зависит от того, в какой степени и насколько удачно она может быть адаптирована к современным технологиям проектирования и производства вычислительных средств. Центральной задачей этой проблемы (назовем ее коротко - проблема адаптации) является задача сокращения «накладных расходов» на реализацию модульных операций. Эти расходы обусловлены тем, что арифметическая операция * (т.е. +, -, ×) над остатками $x, y \bmod p$, как над целыми числами, может приводить к выходу результата операции $x*y$ за диапазон Zp и тогда требуется корректировка результата, т.е. взятие от числа $x*y$ вычета $|x*y|_p$ по $mod\ p$. Операция взятия вычета $|x*y|_p$ выражается формулой:

$$|x * y|_p = x * y - \left\lfloor \frac{x*y}{p} \right\rfloor \cdot p \qquad (1)$$

Эта формула непосредственно связана с аксиомой Архимеда теории действительных чисел, которая предопределяет, так сказать аддитивный характер вычислений с остатками по $mod\ p$.

Технически, реализация операции по этой схеме требует:

а) реализации арифметической операции * над целыми числами x и y;

б) выделения целой части $\left\lfloor \frac{x*y}{p} \right\rfloor$;

в) умножения $\left\lfloor \frac{x*y}{p} \right\rfloor \cdot p$;

г) итогового вычитания, что, собственно, ввиду несоизмеримости модуля p со степенью двойки и приводит к дополнительным расходам.

II. Традиционные пути решения проблемы адаптации. Метод локальной близости оснований к степени двойки

Наиболее распространенным методом адаптации

является выбор оснований модулярной арифметики максимально близкими к степеням двойки. Например, в работах [3], [4], [5] детально изучена система оснований вида $p_1=2^t-1$, $p_2=2^t$, $p_3=2^t+1$. В работах [6], [7] предлагается рассматривать систему оснований вида: $p_1=2^{n1}$, $p_2=2^{n2}-1$, $p_3=2^{n3}-1,\ldots,$ $p_m=2^{nm}-1$, при этом для обеспечения попарной взаимной простоты модулей целесообразно руководствоваться правилом: числа 2^a-1 и 2^b-1 взаимно-простые тогда и только тогда, когда a и b взаимно просты.

Достоинство выбора модулей в виде $p=2^t\pm1$ состоит в том, что все модульные операции по этим модулям над остатками, представленными двоичным позиционным кодом, могут быть получены без формирования величины $\left\lfloor \frac{x}{p} \right\rfloor$, как этого требует формула типа (1). Этот факт следует из тождества:

$$|x|_{2^t\pm1} = \left| |x|_{2^t} \mp \left\lfloor \frac{x}{2^t} \right\rfloor \right|_{2^t-1} \qquad (2)$$

(Здесь, как и выше, символом $|x|_p$ обозначен вычет целого числа x по *mod* p). Как показывает формула (2) шаги б), в), г) вычислений по формуле (1) отсутствуют при вычислениях по формуле (2). По этой причине описанный метод естественно называть методом локальной адаптации арифметики вычетов к бивалентным технологиям.

Обобщением формулы (2) на случай модулей вида $p=2^t\pm k$ служит формула:

$$|x|_p = \left| |x|_{2^t} \mp k \cdot \left\lfloor \frac{x}{2^t} \right\rfloor \right|_p, \qquad (3)$$

которая при специальном выборе параметра k (например, $k=2^s\mp1$, $s<t$) также может обеспечить эффект локальной адаптации. Этот подход приобретает особое значение в тех случаях, когда простое число p – велико. Однако приведенные методы, во-

обще говоря, не устраняют возникновение «накладных расходов», а только лишь смягчают их, ибо для вычисления $|x*y|_p$ необходимо формировать, согласно формуле (1), величину $\left\lfloor \frac{x*y}{2^t} \right\rfloor$, представляющую собой аддитивную избыточность операции * по *mod* 2^t.

III. Исследования в области логарифметики вещественных чисел

Логарифметика поля вещественных чисел R есть арифметика, в которой каждое число представлено его логарифмом (по некоторому фиксированному основанию), а ее операции изоморфны операциям поля R.

Цель перехода к логарифметике: облегчить реализацию мультипликативных операций (умножение и деление) поля R.

Интерес к компьютерной логарифметике возник в конце XX и в начале XXI веков [8], [9]. Однако, если при переходе к логарифмам упрощаются мультипликтивные операции, то несколько сложнее реализуются аддитивные операции. Выигрыш в производительности ожидается лишь при решении специальных задач, в которых число аддитивных операций соизмеримо с числом мультипликативных.

При переходе к логарифметике поля R возникают две трудности (трудности трансляции). Первая трудность состоит в том, что логарифмическая функция определена на пложительных числах: $y = \lg_a x$ ($x > 0$). Распространение традиционных логарифмов на отрицательные числа осуществляется методом симметризации области определения.

В результате центральной симметризации возникает функция:

$$y = \operatorname{sgn} x \lg_a |x| \qquad (1)$$

График этой функции приведен на рис. 1. Область

ее определения задается условием $|x| \neq 0$. Однако, она не является биективной.

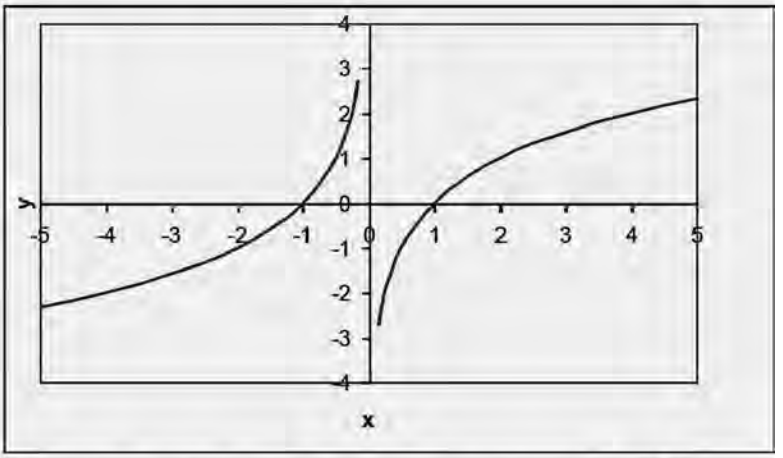


Рис. 1. График функции $y = \operatorname{sgn} x \lg_a |x|$

График ее показывает, что функция (1) имеет две «ветви» взаимной однозначности:

$$y = \begin{cases} \operatorname{sgn} \lg_a |x|, & |x| > 1; \\ 0, & |x| \leq 1. \end{cases} \qquad (2)$$

и

$$y = \begin{cases} 0, & |x| > 1; \\ \operatorname{sgn} \lg_a |x|, & 0 < |x| \leq 1. \end{cases} \qquad (3)$$

Функция (2) задает, так называемый, «расширенный логарифм», определенный на *R*, для которого отрезок *[-1, +1]* представляет «зону нуля», где нарушается условие строгой монотонности. Соответственно, «обратная» функция имеет вид: $y = \operatorname{sgn} x a^{|x|}$, график которой представлен на рис. 2.

Здесь точка $x = 0$ является точкой разрыва непре-

рывности.

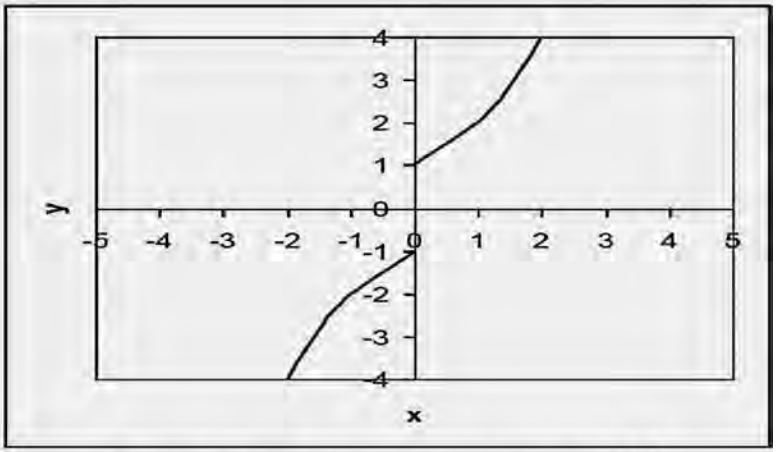


Рис. 2. График функции $y = \operatorname{sgn} x a^{|x|}$

В работе [8] описана логарифметика поля $\mathbb{R}$, построенная на понятии расширенного логарифма (2).

Основное препятствие, которое возникает на пути реализации поля $\mathbb{R}$ это сложность вычисления, так называемого, логарифма Якоби [10], вычисление которого является неотъемлемой частью реализации аддитивной операции в логарифметике. Другое препятствие – это сложность реализации операции округления данных в режиме фиксированной запятой. В этой связи уместно заметить, что, так называемый, режим плавающей запятой также базируется на логарифмическом представлении чисел, а переход к "мантиссам" чисел является оптимальным решением вычислительных проблем логарифметики поля $\mathbb{R}$.

IV. Модулярная логарифметика – преимущества в сравнении с традиционной (позиционной) логарифметикой

Пути преодоления отмеченных выше недостатков

логарифметики поля $\mathbb{R}$ предоставляет модулярная арифметика, получившая широкое распространение у специалистов в области компьютерной арифметики и цифровой обработки сигналов [1], [2].

Для простоты изложения будем считать, что базисные основания $p_1, p_2, \ldots, p_n$ модулярной арифметики являются простыми числами [10].

Впервые модулярную логарифметику в рассмотренном варианте рассмотрел Д. А. Поспелов [12]. Здесь для упрощения мультипликативных операций модулярной арифметики используется традиционный подход – переход от вычетов к логарифмам (индексам). Однако ему присуща разбалансировка между затратами на аддитивные и мультипликативные операции. А именно, мультипликативная операция помимо аддитивной операции по *mod (p-1)* требует двух операций преобразования: а) от вычета (остатка) к индексу (логарифмирование), б) от индекса к вычету (антилогарифмирование).

Чтобы сбалансировать модульные операции Д. А. Поспелов предложил каждый вычет $|x|_{p_i}$ представлять парой $<|x|_{p_i}, \lg|x|_{p_i}>$, т.е. точкой на логарифмике - графике функции $y = \left|\lg|x|_p\right|_{p-1}$ (сингулярное значение логарифма при $|x|_p = 0$ распознается по первой компоненте пары). В таком случае все модульные операции как подчеркивает Д.А. Поспелов, приобретают однотипность. А именно, пусть $\alpha_x = <|x|_p, \lg|x|_p>$, $\alpha_y = <|y|_p, \lg|y|_p>$, тогда аддитивные и мультипликативные операции реализуются по однотипным схемам:

1) аддитивная операция:

$$z := \left||x|_p \pm |y|_p\right|_p \xrightarrow{\lg} \lg z \rightarrow < z, \lg z >$$

2) мультипликативная операция:

$$z := \left|\lg|x|_p + \lg|y|_p\right|_{p-1} \xrightarrow{\lg^{-1}} < \lg^{-1}(z), z >$$

(Здесь операции lg и $\lg^{-1}$ суть логарифмирование и

потенцирование).

Источником накладных расходов такого подхода служит удвоение регистров операндов. Адаптацию к бивалентным технологиям здесь можно усмотреть по двум обстоятельствам: все модульные операции сведены к сумматорам двух типов - по $mod\ p_i$, $mod(p_i-1)$, при этом модули (p_i-1) разлагаются на более мелкие множители, благодаря чему достигается большая технологичная близость к степени двойки в сравнении с модулем p_i. В криптографии простые числа p такие, для которых $(p-1)$ разлагаются на более, чем два простых сомножителя, называются гладкими. Естественно, число простых сомножителей числа $(p-1)$ назвать степенью гладкости простого числа p. В класс арифметических задач модулярной арифметики, чем выше гладкость ее простых базисных модулей p_i, тем выше их технологичность, т.е. тем более модулярная арифметика оказывается адаптированной к бивалентным технологиям [13].

Приведенные выше примеры показывают, что «накладные расходы» на модульные операции обусловлены аддитивной природой целых чисел, источником которой служит аксиома Архимеда. Она же предопределяет аддитивный характер всех арифметических вычислений. В частности, в рамках модулярной арифметики все немодульные операции существенно обусловлены аддитивной природой чисел.

В свете сказанного можно утверждать, что позиционная система счисления (в отличие от непозиционной) максимально адаптирована к аддитивной природе целых чисел или, точнее, адекватна их аддитивной природе.

Для совершенствования адаптации модульных операций модулярной арифметики к бивалентным технологиям имеется еще один путь – отказаться на уровне модульных операций от аддитивных вычислений и перейти к мультипликативным (т.е. логарифметическим).

В строгом смысле под термином модулярная лога-

рифметика кольца $\mathbb{Z}_{p_1 p_2 \dots p_n}$ понимается арифметика кольца, порождаемая прямым произведением логарифметик полей Галуа $GF(p_i)$ $(1 \le i \le n)$ [9].

Логарифметика поля $GF(p)$ разработана выдающимися математиками К. Ф. Гауссом, К. Г. Я. Якоби и их последователями в первой половине XIX [10], [14].

Эта арифметика является расширением индексной арифметики поля $GF(p)$ на сингулярную точку (т.е. нулевую точку поля $GF(p)$). Операции логарифметики конструируются так, чтобы логарифметика поля $GF(p)$ была изоморфна арифметике конечного поля $GF(p)$.

Рассмотрим дискретный логарифм над полем GF(p), определенный по формуле:

$$\lg_w |x|_p = (2^t - 1)\delta(|x|_p) + ind_w |x|_p \, \hat{\delta}(|x|_p) . \qquad (5)$$

Здесь:

- $\delta(|x|_p) = \begin{cases} 1, |x|_p = 0, \\ 0, |x|_p \neq 0; \end{cases}$

- $t = \lceil lg_2(p) \rceil$ - битность модуля p, где $\lceil \alpha \rceil$ - наименьшее целое число, превосходящее α ;

- $\hat{\delta}(|x|_p)$ - кофункция Кронекера, т.е. $\hat{\delta}(|x|_p) = 1 - \delta(|x|_p)$;

- w – примитивный элемент поля GF(p);

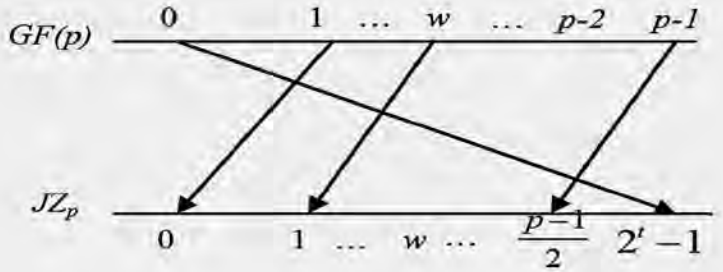
- $ind_w |x|_p$ - индекс вычета $|x|_p$ по основанию w, т.е.

$$|x|_p \neq 0 \Leftrightarrow \left| w^{ind_w |x|_p} \right|_p = |x|_p$$

- $|x|_p = 0$ - точка сингулярности логарифма.

Замечание. Выбор показателя t символа сингулярности $2^t - 1$ экономичен тем, что он не увеличивает числа бит для своего представления в сравнении с битностью двоичного представления элементов поля GF(p) и имеет стандартную форму для любого простого числа p.

Согласно определению, расширенный логарифм $y = \lg_w |x|_p$ взаимнооднозначно отображает поле *GF(p)* на множество $JZ_p = \{0,1,2,...,p-2,2^t-1\}$. Характерными точками этого отображения являются точки *0, 1, w, p-1* $\in GF(p)$, которые при любом простом $p>2$ и любом w отображаются соответственно в точки $2^t-1, 0, 1, \frac{p-1}{2} \in JZ_p$:



В силу биективности функция $y = \lg_w |x|_p$ порождает на JZ_p структуру поля, изоморфную полю *GF(p)*.

Обозначим символами $\boxplus$ $\boxtimes$, соответственно, аддитивную и мультипликативную операции поля JZ_p.

Согласно определению, если $\alpha = \lg_w |a|_p$, $\beta = \lg |b|_p$, то

$$\alpha \boxplus \beta = \lg_w |a \cdot b|_p,$$

$$\alpha \boxtimes \beta = \lg_w |a + b|_p$$

Процедура изоморфного конструирования операции логарифметики поля GF(*p*) описана в трудах [15], [16], [17]. Существенно, что они включают в себя процедуры взаимодействия с сингулярными значениями расширенного логарифма, в отличии от индексной арифметики, рассмотренной в [17], где ис-

ключены из вычислений взаимодействия с сингулярными точками области определения и сингулярными значениями области значений дискретного логарифма.

Обозначим символом $\mathcal{L}_p$ логарифметику поля GF(p). По построению $\mathcal{L}_p$ является полем изоморфным полю GF(p). Следовательно, модулярная логарифметика $\mathcal{L}_{p_1} \times \mathcal{L}_{p_2} \times \ldots \times \mathcal{L}_{p_m}$ изоморфна модулярной арифметике кольца $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_m}$.

Главное достоинство модулярной логарифметики $\mathcal{L}_{p_1} \times \mathcal{L}_{p_2} \times \ldots \times \mathcal{L}_{p_m}$ в сравнении с традиционной состоит в том, что она позволяет преодолеть барьер пиковой разрядности логарифметики $\mathbb{Z}_{2^n}$, возникающий в связи с возрастанием сложности вычисления логарифмов Гаусса – Якоби с возрастанием n. Модулярная арифметика позволяет преодолеть этот барьер при больших n за счет организации параллельных логвычислений в малых диапазонах чисел по малым диапазонам модулей кольца $\mathcal{L}_{p_1} \times \mathcal{L}_{p_2} \times \ldots \times \mathcal{L}_{p_m}$.

При этом выполняется условие:

$$p_1\, p_2 \ldots p_m > 2^n$$

Другие достоинства модулярной логарифметики слогаются из того, что она открывает новые технологичные возможности для совершенствования всех процедур модулярной арифметики. Рассмотрим (бегло) некоторые из них.

1. Технически все модульные операции по каждому модулю p логарифметики имеют одинаковую структуру, т.е. состоят из трех цифровых блоков:
   - простых булевых схем - идентификации сингулярности (так называемые, предикаторы сингулярности);
   - сумматоров по модулю p – 1;
   - одновходовых таблиц Якоби.

   Совокупно эти блоки объединяются в, так называемый, вычислительный элемент (ВЭ). В зависимости от функциональной принадлежности, ВЭ может иметь различную архитектуру.
2. Вычислительный элемент допускает универсали-

зацию относительно семейства однотипных модулей $p_1, p_2, \ldots, p_n$. Семейство модулей $p_1, p_2, \ldots, p_n$ однотипно, если $[p_1 - 1, p_2 - 1, , \ldots, p_n - 1]$ (практически) близко по порядку к максимальному модулю.

Универсальные вычислительные элементы составляют базу для построения надёжных архитектур модульных вычислений.

3. Универсальный вычислительный элемент, наделенный системой кодовой защищенности, является внутренним самокорректирующим элементом модулярной вычислительной системы. Кроме того сам модулярный код является самокорректирующимся. Таким образом, кодовая защищенность вычислителя модулярной логарифметики представляет собой прямое произведение двух типов кодовой защищенности: внутренней и внешней. Это открывает перспективы для разработки высоконадежных вычислительных структур на основе кодовой защищенности, с одной стороны, и для разработки теоретических исследований, связанных с распространением идей и методов теории К. Шеннона достоверной передачи информации по каналам связи с шумом на надежность вычислительных каналов с шумом. Точнее, расширить классические исследования Винограда С. и Коэна Дж. Д., «Надежные вычисления при наличии шумов», М., Наука, 1968, 112 с., на случай шумящих каналов арифметической обработки данных.
4. Оптимальный выбор технологичных модулей и разработка библиотек функциональных блоков модулярной логарифметики для САПР Synopsys. Эта задача корректно ставится лишь в рамках модулярной логарифметики.
5. Разработка принципов конвейерной реализации всех немодульных операций модулярной логарифметики.
6. Выбор технологичных модулей p вида $4k + 1$ (в силу теоремы Гаусса об изоморфизме) позволяет все достоинства модулярной логарифметики ве-

щественно-значных величин распространить на модулярную логарифметику комплексно-значных величин. Таким образом, достигается расширение среды параллельных логвычислений над вещественными величинами на компьютерную арифметику логвычислений над комплексно-значными величинами.

7. Модулярная логарифметика впервые позволяет ставить задачу об эффективной адаптации модулярной арифметики к бивалентным технологиям проектирования методом варьирования выбора "гладких" технологичных модулей.
8. Разработка реконфигурируемых арифметических структур конвейерного типа и параллельного действия.
9. Разработка устройств быстрых линейных преобразований, а также устройств быстрых и надежных операций матричной алгебры. [18]

V. Заключение

Модулярная логарифметика не снимает трудностей аппаратной и временной реализации таких немодульных операций как округление, формирование знака числа, перевода двоичных кодов в модулярный и обратно, и других. Однако, позволяет глубже взглянуть на особенности надежных модулярных вычислений при наличии шумов в модульных каналах; позволяет строить оптимальные в смысле минимизации бивалентного дефекта модульные структуры вычислителей различного рода, используемых в системах цифровой обработки сигналов; позволяет эффективнее использовать идеи паралеллизма и организации вычислений, но уже на уровне машинных кодовых слов, заложенных в трудах отечественных ученых [19] – [22].

VI. Литература

[1] Soderstrand M.A., Jenkins W.K., Jullien G.A., and Taylor

F.J. Residue Number System Arithmetic: Modern Applications in Digital Signal Processing // IEEE Press, 1986.
[2] Юбилейная Международная научно-техническая конференция «50 лет модулярной арифметике»: Сб. научных трудов. М.: ОАО «Ангстрем», МИЭТ, 2006. 775 с.
[3] Корнилов А.И., Семенов М.Ю., Ласточкин О.В. // Принципы построения модулярных индексных умножителей. – Известия ВУЗов. Электроника. 2004. №2.
[4] Амербаев В.М., Стемпковский А.Л., Широ Г.Э. Модулярный быстродействующий согласованный фильтр // «50 лет модулярной арифметике»: Сб. научных трудов. М.: ОАО «Ангстрем», МИЭТ, 2006. С. 250 – 267.
[5] Корнилов А.И., Семенов М.Ю., Ласточкин О.В., Калашников В.С. Применение современных методов проектирования при реализации модулярных вычислительных процедур // «50 лет модулярной арифметике»: Сб. научных трудов. М.: ОАО «Ангстрем», МИЭТ, 2006. С. 369 – 383.
[6] Parhomi B., Computer arithmetic: algorithm and Hardware designs // Oxford University Press, 2000. № 4.
[7] Koren J., Computer Arithmetic Algorithms – Massachusetts, 2002.
[8] Шауман А.М., Основы машинной арифметики. – Ленинград: изд. ЛГУ, 1979.
[9] Arnold M.G., Residue Logarithmic number System, Theory and Implementation // Computer Arithmetic, 27-29 June 2005. P. 196-205.
[10] Лидл Р., Нидеррайтер Г. Конечные поля: в 2 т. / под общ. ред. В.И. Нечаева. М.: Мир, 1988.
[11] Виноградов И.М. Основы теории чисел. М.: Наука, 1972.
[12] Поспелов Д.А. Арифметические основы вычислительных машин дискретного действия. М.: Высш. шк., 1970.
[13] Амербаев В.М., Константинов А.В., Тельпухов Д.В. Бивалентный дефект модулярных кодов // Проблемы разработки перспективных микро- и наноэлектронных систем – 2008. Сб. научных трудов / под общ. ред. А.Л. Стемпковского. М.: ИППМ РАН, 2008. С. 462- 466.
[14] Математический Энциклопедический словарь. М.: Сов. энциклопедия, 1988. С. 141, 330.
[15] Zelniker G., Taylor F.J., A Reduced Complexity Finite Field ALU // JEEE Truns. Sirc. Syst. Dec. 1991. V. 38.
[16] Williams T.A. Circuit for Adding and/or Substracting Representation – U.S. Patent, № 4, 727, 508. Feb.23 1988.
[17] Preethy A.P., Padhakrishnan D. An RNS based logarithmic adder // JEEE Proceeding, Computer and Digital Tech-

niques. July, 2000. V. 147, Issue 4. P. 283–296.
8] Виноград С., Коуэн Дж. Д. Надежные вычисления при наличии шумов. М.: Наука, 1968. 112 с.
9] Воеводин В.В. Вычислительная математика и структура алгоритмов. М.: Изд. МГУ, 2006.
0] Современные проблемы вычислительной математики и математического моделирования: в 2 т. / Т. 1: Вычислительная математика, Т. 2: Математическое моделирование. М.: Наука, 2005.
1] Бурцев В.С. Параллелизм вычислительных процессов и развитие архитектуры Супер ЭВМ. М.: Торус Пресс, 2006. 416 с.
2] А.Л.Глебов, Гурарий М.М., Егоров Ю.Б., Жаров М.М., Русаков С.Г., Ульянов С.Л., Стемпковский А.Л. Актуальные проблемы моделирования в системах автоматизации схемотехнического проектирования // под. общ. ред. Стемпковского А.Л. М.: Наука, 2003. 430 с.

Факсимильное издание.
Опубликовано в сборнике научных трудов
IV Всероссийской научно-технической конференции
«Проблемы разработки перспективных микро- и наноэлектронных систем — 2010». —
Москва: ИППМ РАН, 2010. — С. 368–373.

Модулярная арифметика сегодня[1]

Амербаев В. М.

Привлекательные структурные особенности модулярной арифметики — параллелизм и распределённость арифметических операций на уровне операндов, а также арифметичная самокоррекция, потенциально обуславливающие высокую производительность и надёжность вычислений, оборачиваются (вследствие бивалентности современных технологий проектирования и производства вычислительных средств) недостатками субструктурных характеристик модульных операций. Это выражается в увеличении «накладных расходов» на реализацию:

[1] Статья была написана в 2013 г.

- модульных операций вследствие несоизмеримости оснований модулярной арифметики со степенью двойки (т.н. бивалентный дефект модулярной арифметики),
- всех немодульных операций, включая процедуры обнаружения и исправления ошибок, вследствие их кодовой незащищённости от сбоев и отказов.

Трудности борьбы с этими недостатками были одной из причин временного спада интереса к модулярной арифметике после успешного её старта в 1950–1960-е годы.

История развития компьютерной техники, как в нашем Отечестве, так и за его пределами, в части использования модулярной арифметики характеризуется многообразием теоретических исследований по минимизации этих «накладных расходов» и прикладных решений задач проектирования на их основе. Эти исследования в конце XX столетия получили новый стимул для дальнейших разработок, который явно формулируется как проблема «адаптации модулярной арифметики к двоичной арифметике». Иными словами, требуется разработать оптимальные двоичные реализации модульных вычислений по каждому модулю модулярной арифметики.

Острота этой проблемы на текущий момент обусловлена тотально господствующим положением двоичной арифметики как в технологиях микроэлектроники, так и в мире систем автоматизации проектирования цифровых устройств.

В связи с этим в ИППМ РАН его директором академиком РАН А. Л. Стемпковским была поставлена поисковая проблема — адаптация модулярной арифметики к бивалентным технологиям микроэлектроники и преодоление на этой основе факторов возникновения «накладных расходов» в классе задач повышения надёжности вычислений. Такая постановка требовала отказа от традиционного понимания остатков (вычетов). Это оказалось возможным в общей схеме логарифмических вычислений. В связи с этим отметим, что на стыке XX–XXI веков и за рубежом, и в России интенсивно прорабатывалась компьютерная логарифметика, где числа изображались парой — знаком числа и логарифмом абсолютной величины этого числа. При подобном «мультипликативном» представлении чисел

сильно упрощаются операции деления и умножения, но усложняется цифровая реализация аддитивных операций (сложение и вычитание чисел, представленных их логарифмами, т. е. возникает проблема ускорения вычисления так называемого логарифма Гаусса). Последнее существенно упрощается переходом к так называемому логарифму Якоби. Но сама проблема вычисления дискретного логарифма по своей природе остаётся вычислительно сложной, а прямое табличное её решение ограничено объёмом используемой памяти компьютера (для 32-разрядных операндов требуются таблицы порядка 10^{32} бит), т. е. возникает «проклятие размерности».

Математикам давно известно (уже порядка 200 лет), что подобная схема логарифметики имеет место для любых полей, в частности и для конечных. В этом плане модулярная арифметика позволяет преодолеть «проклятие размерности», если в качестве оснований p_i модулярной арифметики избрать малобитные простые числа и использовать логарифмическое представление вычетов по каждому простому основанию p_i. Таким образом, возникает возможность распространить технологию логарифмических вычислений над многобитным диапазоном на кольцо вычетов целых чисел по составному модулю $P = p_1, p_2, ..., p_n$ и получить прямое произведение малобитных «логарифметик», изоморфное традиционной модулярной арифметике многобитного диапазона по модулю $P = p_1, p_2, ..., p_n$. Возникли понятия:

- модулярный LG-код, адекватный традиционному модулярному коду,
- модулярная логарифметика.

В рамках модулярной логарифметики удалось:

- разработать пути сокращения «накладных расходов» на модульные и немодульные операции,
- существенно сократить, в сравнении с традиционной реализацией модулярной арифметики, временные и аппаратные затраты на все типы арифметических операций,
- разработать новый тип архитектуры модулярного процессора,

- разработать новую форму кодовой защиты от помех всех процедур, как модульных, так и немодульных.

Это достигается посредством специального выбора простых оснований с требуемой внутренней структурой, диктуемой адаптацией к бивалентным технологиям. Исследуются алгоритмы вычислительной алгебры в сигнатуре логарифметики, задачи ускорения ортогональных преобразований, в частности дискретного преобразования Фурье тригонометрического базиса. Следует отметить, что если в традиционной арифметике схема БПФ формируется посредством сокращения числа операций умножения (как более трудоёмкой, чем сложение), то в логарифметике ситуация диаметрально противоположная, т. к. здесь более трудоёмкими оказываются аддитивные операции над числами, представленными их логарифмами.

Предварительная проработка показала, что достаточно эффективное решение проблемы адаптации модулярной арифметики оказалось возможным на путях спецификации выбора оснований модулярной арифметики.

Возникли следующие тенденции:

- выбор оснований, «близких» к степеням двойки,

- выбор в качестве оснований простых чисел p, таких, чтобы числа $p-1$ удовлетворяли критериям адаптации, — так называемые гладкие простые числа.

В настоящее время в ИППМ РАН в рамках «проблемы адаптации» разрабатываются:

- бимодульная модулярная арифметика, базирующаяся на бимодульной арифметике конечного поля Гаусса GF(p), идея которой была впервые высказана профессором Д. А. Поспеловым в 1970 году;
- рекурсивная модулярная арифметика, сводящая операции модулярной арифметики к операциям по однотипным малобитным основаниям, идея построения которой была предложена академиком РАН А. Л. Стемпковским в 2010 г.;
- модулярная логарифметика, базирующаяся на прямом произведении логарифметик конечных полей Галуа GF(p).

Результаты исследований в этих направлениях позволили по-новому взглянуть на такие проблемы, как:

- разработка нетрадиционных архитектур модулярных процессоров,
- разработка высокоскоростных и высоконадёжных модулярных вычислителей,
- разработка принципов построения энергосберегающих модулярных вычислителей.

В этом плане модулярная арифметика становится вполне конкурентоспособной двоичной, а в ряде случаев, например:

- вычисления в алгебре матриц над полем вещественных чисел R,
- вычисления над полем комплексных чисел C,
- вычисления над телом кватернионов Q,

модулярная арифметика имеет существенные преимущества.

При этом, однако, кардинальным остаётся требование, чтобы все упомянутые вычисления велись в режиме фиксированной запятой, что в общем случае благоприятствует повышению точности вычислений в сравнении с вычислениями в режиме с плавающей запятой.

Повышение эффекта вычислений над комплексными и гиперкомплексными числами достигается на основе теоремы Гаусса об изоморфизме, которая позволяет получить более глубокое распараллеливание модулярных вычислений в кольце гауссовых чисел. Теорема Гаусса не имеет аналога в двоичной арифметике.

Таким образом, логарифметика открывает новые технические возможности использования достижений современных бивалентных технологий в задачах проектирования модулярных вычислительных средств специального назначения. На существующих средствах проектирования и полупроводниковых технологиях она обеспечивает возможность практического создания унифицированных IP-блоков:

- быстродействующих специальных устройств цифровой обработки сигналов модулярного типа в сигнатуре логарифметики,

- высоконадёжных устройств модулярной логарифметики, способных выступать в роли арифметических блоков «автономного компьютинга».

Хочется заметить, что идея модулярных вычислений была привнесена в Россию в начале шестидесятых годов прошлого столетия крупным советским учёным и организатором науки профессором Федором Викторовичем Лукиным, который первым организовал исследовательские работы в области модулярных вычислений. Привлекательной на то время была возможность табличной реализации в рамках модулярной арифметики мультипликативных операций. Он обратил внимание профессора И. Я. Акушского на зарубежные исследования в области модулярной арифметики и, став первым директором зеленоградского Центра микроэлектроники, организовал Специализированный вычислительные центр (СВЦ), а директором СВЦ назначил ученика И. Я. Акушского кандидата технических наук Давлета Исламовича Юдицкого, имевшего к тому времени опыт разработки специализированного модулярного компьютера. Однако безвременная кончина Федора Викторовича, лишившая Д. И. Юдицкого высокого покровительства, не позволила в условиях советской тоталитарной государственности эффективно продолжать разработки, начатые в СВЦ. Тем не менее семена модулярной арифметики, брошенные Ф. В. Лукиным на плодородную интеллектуальную почву страны, и популяризаторская деятельность профессора И. Я. Акушского быстро взросли и распространились по Союзу.

Образовались научные коллективы в области модулярной арифметики по различным городам Союза, многие из которых успешно действуют и поныне. В настоящее время в России и на территории бывшего Союза знамя, поднятое Д. И. Юдицким в области проектирования модулярных процессоров, поддерживается:

- в Москве — ИППМ РАН, возглавляемого академиком РАН Стемпковским А. Л.;
- в Алма-Ате (Республика Казахстан) в Институте проблем информатики и управления МОН РК, возглавляемого профессором, членом-корреспондентом НАН РК

М. Н. Калимолдаевым, где исследуются принципы модулярных вычислений в кольце полиномов над произвольным полем, а также над полем комплексных чисел и над полем гауссовых чисел;

- в Минске (Белоруссия) в НИИ прикладных физических проблем им. А. Н. Севченко БГУ, возглавляемого профессором, академиком НАН Белорусии А. Ф. Чернявским, где успешно решаются проблемы современной компьютерной модулярной арифметики в различных прикладных направлениях, спроектирован и разработан ряд модулярных процессоров специального назначения;
- в городе Ставрополе в Ставропольском военном институте связи ракетных войск, где профессор Н. И. Червяков возглавляет большую научно-техническую школу, которая решает проблемы модулярной арифметики на платформе нейрокомпьютерных технологий.

Островки научных исследований в области модулярной арифметики представлены в многочисленных исследовательских центрах и вузах страны. Подробная информация об этих организациях отражена в сборнике научных трудов юбилейной международной научно-технической конференции «50 лет модулярной арифметике» в рамках V международной научно-технической конференции «Электроника и информатика — 2005 (Москва, ОАО «Ангстрем», МИЭТ, 2006. — 775 с.).

Все это говорит о том, что модулярные аспекты компьютерных технологий привлекают внимание большого круга специалистов в области проектирования вычислительных средств, набирая новые обороты.

В личном плане хочу сказать, что мои работы в области модулярной арифметики я связываю с большим влиянием на меня и на мое творчество талантливого инженера, учёного и организатора работ в области новаторских решений проблем конструирования вычислительных средств д. т. н., профессора Давлет-Гирея Ислам-Гиреевича Юдицкого, который своим ярким примером беззаветного служения Отечеству отдал свой талант новому научно-техническому направлению — созданию вычислительных структур параллельного действия, открыл

своим коллегам просторы для исследований и разработок высоконадёжных и высокоскоростных специализированных вычислительных устройств.

Опубликовано в книгах:

- *«50 лет отечественной микроэлектронике. Краткие основы и история развития». — М.: Техносфера, 2013. — С. 441–448.*
- *История отечественной вычислительной техники». — М.: Столичная энциклопедия, 2014. — С. 200–201.*
- *История отечественной вычислительной техники». Изд. 2. — М.: Столичная энциклопедия, 2017. — С. 242–243.*

Принципы рекурсивных модулярных вычислений

Стемпковский А. Л., Амербаев В. М., Соловьёв Р. А.

Предложен новый метод, который базируется на идее выразить систему модулей традиционной модулярной арифметики через систему субмодулей, имеющую меньшую размерность. Новое рекурсивное представление данных позволяет устранить часть известных недостатков модулярной арифметики. Несмотря на ограничения, которые накладываются на систему модулей, предложенный метод, как показывают эксперименты, обеспечивает выигрыш по скорости и может быть применён в параллельных высокоскоростных вычислительных устройствах.

Ключевые слова: модулярная арифметика, параллельные вычисления, система остаточных классов.

1. Введение в рекурсивную модулярную арифметику

В настоящей статье рассматривается развитие некоторых конструктивных идей, которые были изложены одним из соавторов в докладе «Рекурсивная модулярная арифметика» в сентябре 2010 года на учёном совете ИППМ РАН и представлены в обобщённой схеме в патенте на полезную модель [1].

В истории вычислительной техники известны случаи, когда при проектировании специализированных устройств не удавалось эффективно обеспечить нужные быстродействие

и надёжность, используя обычную позиционную (двоичную) арифметику. В то же время использование модулярных вычислений позволяло решить проблему. Модулярная арифметика не является универсальным способом построения вычислителей, но в некоторых специализированных применениях она незаменима. В связи с этим интерес к ней не угасает вот уже многие десятилетия. Результаты исследований, которые позволили бы преодолеть её недостатки и расширить область её применения, постоянно публикуются, практически существует целое научное направление, которое занимается этим вопросом [2–5].

Известны преимущества, которые даёт использование модулярной арифметики при проектировании вычислителей:

1) естественный параллелизм вычислений,
2) возможность самоконтроля и исправления неисправностей.

Известны также и её недостатки:

1) большие накладные расходы (наличие преобразователей из позиционного кода в модулярный и обратно);
2) представление модульных операций через операции позиционной двоичной арифметики, что приводит к избыточности оборудования при их реализации;
3) неравномерность (неоднородность) модульных вычислителей по сложности и времени выполнения операций;
4) отсутствие должной поддержки проектирования модулярных вычислителей устройств со стороны САПР (средств структурного синтеза).

Первый недостаток может быть нивелирован, если проектируются достаточно сложные вычислители. Поскольку аппаратные затраты преобразователей ограничены проектными нормами, то, увеличивая сложность устройства в целом, можно снизить долю накладных расходов. То же самое можно сказать и о временных затратах.

Четвёртый недостаток может быть преодолён использованием так называемых IP-генераторов — программных модулей, производящих поведенческое синтезируемое описание на уровне RTL-устройств, выполняющих те или иные модулярные (возможно, и не модулярные) процедуры.

О каких-либо существенных способах по преодолению второго и третьего недостатков неизвестно. На преодоление именно этих недостатков направлен новый подход к проектированию модулярных вычислителей, который назван «рекурсивная модулярная арифметика».

Идеи, предложенные в настоящей статье, основаны на принципе глубокого распараллеливания модульных операций модулярной арифметики с основаниями $p_1, p_2, ..., p_n$ посредством редуцирования модульных операций по каждому рабочему основанию $p_i (i \le j \le n)$ к модульным вычислениям по предшествующим рабочим основаниям $p_1, p_2, ..., p_{i-1}$, имеющим то или иное технологическое преимущество (например малобитным), которые будем называть базисными основаниями. При этом упомянутая редукция допустима только при выполнении так называемого условия согласования вычислительных диапазонов по каждому рабочему модулю p_i с вычислительными диапазонами по соответствующим комплексам базисных оснований. Принцип согласования гарантирует, во-первых, изоморфизм кольцевых операций по соответствующим им комплексам базисных оснований и, во-вторых, выполняемость обращения каждого шага рекурсии посредством перевода соответствующих модулярных кодов в позиционный код по базисным основаниям (например на основе китайской теоремы об остатках или переводом их в полиадический код).

2. Идея рекурсивной модулярной арифметики

Поясним процедуру рекурсивных преобразований на простом примере. Возьмём в качестве базисных модулей двухбитные простые числа $p_1 = 2$, $p_2 = 3$. Очевидно, что вычетами по модулям 2 и 3 можно однозначно представить любой вычет по модулю 5. В то же время вычетами по модулям 2, 3 и 5, где вычеты по модулю 5 представимы по модулям 2 и 3, можно однозначно представить любой вычет по модулю 29. Вычетами по модулям 2, 3, 5 и 29 можно однозначно представить любой вычет по модулю 863. И так далее, пока не получим нужный набор рабочих оснований: 2, 3, 5, 29, 863 ... — Данный пример наглядно иллюстрирует четыре факта:

1) аппаратные и временные затраты на представление чисел по базовым модулям 2 и 3 примерно одинаковы (оба базисных модуля двухбитные);
2) наблюдается более высокая степень распараллеливаемости;
3) появляется регулярность (все вычисления по модулям 2 и 3);
4) столь малая разрядность базовых модулей позволяет эффективно реализовать модульные операции по базисным модулям в комбинационных схемах.

На самом деле не всё так красиво. Реально существует ряд ограничений, которые надо выполнять и которые приводят к усложнению устройств, выполненных по предлагаемой методологии. Рассмотрим эти ограничения.

Пусть имеем систему базисных модулей (p_1, p_2, ..., p_m) и необходимо представить вычеты по модулю p_{m+1} через вычеты по упомянутой системе базовых модулей. Очевидно, что максимальный вычет по модулю p_{m+1} равен $max = p_{m+1} - 1$. Зная это значение и последовательность выполняемых операций, можно рассчитать максимальное значение MAX результата арифметической операции. Очевидно, что для однозначного представления результата арифметических операций необходимо, чтобы $MAX < Q$, где $Q = p_1 \cdot p_2 \cdot \ldots \cdot p_m$. Для остальных модулей расчёт производится аналогично.

Вернёмся к нашему примеру с базовыми модулями 2 и 3. В этом случае $Q = 2 \cdot 3 = 6$. Наименьшее простое число (после 2 и 3, конечно) есть 5 ($max = 4$). Мы не можем выполнить ни операцию сложения, т. к. $2 \cdot max > Q$ ($8 > 6$), ни тем более операцию умножения, т. к. $max^2 > Q$ ($16 > 6$). Чтобы выполнить любую из арифметических операций (сложение или умножение), нам необходимо увеличить число Q (увеличить значения базисных модулей и/или их количество). Возьмём в качестве базисных модулей все взаимно простые трёхбитных числа: 4, 5 и 7. В этом случае $Q = 4 \cdot 5 \cdot 6 = 140$. Чтобы имело место $MAX < Q$, для операции умножения необходимо выполнение условия $max^2 < Q$ или $p_{i-1} < \sqrt{Q}$ ($p_{i-1} < 11{,}8$). Таким образом, выбираем $p_i = 11$

(ближайшее к 7 простое число). Далее совокупность рабочих модулей строится без каких-либо проблем с помощью аналогичного расчёта, пока не будет достигнут требуемый вычислительный диапазон.

Наконец, рассмотрим реальный случай. Пусть нам нужно реализовать преобразователь Фурье для 24-битных аргументов при количестве точек 1024. Для этого потребуется вычислить сумму 1024 произведений, т. е. обеспечить $1024 \cdot \max^2 < Q$. Здесь уже не обойтись системой только трёхбитных базисных модулей. Добавим к ним четырёхбитные: 5, 7, 8, 9, 11 и 13 (Q = 360360). Для выбора ближайшего рабочего модуля необходимо $p_i - 1 < \sqrt{\frac{Q}{1024}}$. Получаем $p_i - 1 < 32$. Выбираем $p_i = 31$. Аналогичным расчётом реализуем рекурсивное дерево рабочих оснований целиком. Чтобы сделать такое устройство, нужно спроектировать блок из шести вычислителей (для каждого базисного модуля), и таких блоков нужно будет 16. Вот, где работает регулярность. Заметим, что все вычислители будут иметь высокую скорость модульных операций (суперраспараллеливание) и небольшие аппаратные затраты в силу малости базисных модулей или их близости к степеням двойки.

Таким образом, предложенный аппарат рекурсивных модулярных вычислений даёт следующие преимущества:

- устранение дисбаланса в операциях с малыми и большими модулями (аппаратные и временные затраты примерно одинаковы, т. к. в идеале все базисные модули имеют одинаковое число битов);
- существенно более высокая степень распараллеливаемости, а значит, и более высокое быстродействие;
- появляется регулярность (большое количество одинаковых базисных модулей);
- малая разрядность базисных модулей позволяет реализовать модульные операции на комбинационных схемах, оптимизированных в базисе булевых функций.

3. Представление данных и основные операции в рекурсивной модулярной арифметике

Идея, на которой базируется рекурсивная модулярная арифметика, — выразить систему модулей через систему субмодулей, имеющую меньшую размерность.

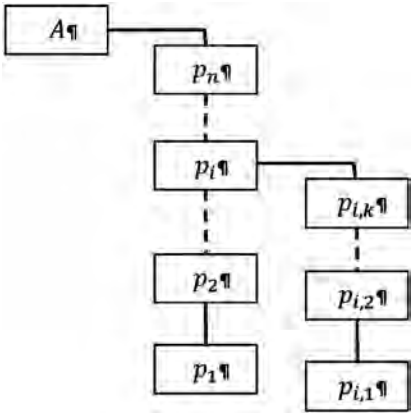


Рис. 1. Иерархия в модулярной арифметике

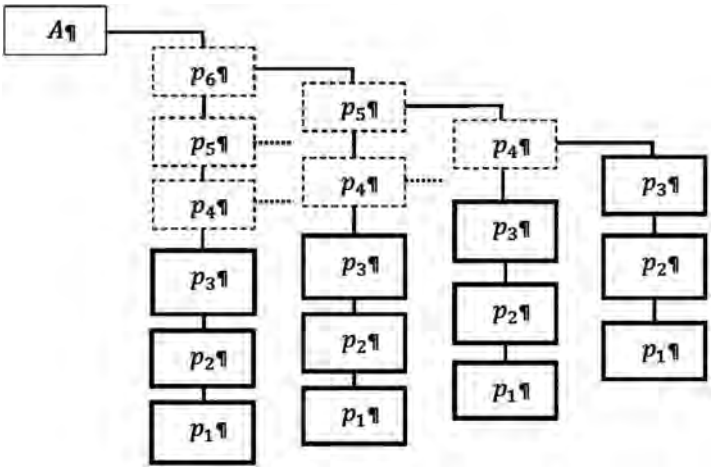


Рис. 2. Рекурсивное разложение элемента p6 через систему субмодулей (p1, p2, p3)

Пусть задана система модулей (p_1, p_2, ..., p_i, ..., p_n) и задан некоторый вектор $A = (a_1, a_2, ..., a_n)$. Выразим a_i через систему субмодулей ($p_{i,1}, p_{i,2}, ..., p_{i,k}$), где $P_i = p_{i,1} \cdot p_{i,2} \cdot ... \cdot p_{i,k}$ и $a_i < P_i$: $a_i = (a_{i,1}, a_{i,2}, ..., a_{i,k})$. В этом случае вектор A можно представить в следующем виде: $(a_1, a_2, ..., a_{i-1}, (a_{i,1}, a_{i,2}, ..., a_{i,k}), a_{i+1}, ..., a_n)$ (рис. 1).

Назовём систему из m младших модулей системой базовых модулей, а их произведение обозначим $Q = (p_1 \cdot p_2 \cdot ... \cdot p_m)$. Пусть $p_{i,1} = p_i$, $p_{i,2} = p_2$, ..., $p_{i,i-1} = p_{i-1}$, а $k = i - 1$, тогда при $i = m + 1$, ..., n имеет место рекурсия: $a_i = (a_1, a_2, ..., a_m, a_{m+1}, ..., a_{i-1})$ по системе модулей p_1, p_2, ..., p_m, p_{m+1}, ..., p_{i-1} или, раскрывая рекурсию: $a_i = (a_1, a_2, ..., a_m, (a_{m+1,1}, a_{m+1,2}, ..., a_{m+1,m}), ...)$. На рис. 2 приведён частный случай разложения элемента a_i для случая, когда $n = 6$ и $m = 3$.

3.1. Прямое преобразование числа в позиционной системе счисления в представление в рекурсивной модулярной арифметике

Если в традиционной модулярной арифметике число элементов вектора равно числу элементов в системе модулей, то в рекурсивной модулярной арифметике количество элементов вектора увеличивается в зависимости от заданных n и m.

Очевидно, что каждый из первых m элементов представляется в виде одного числа; $m + 1$-элемент содержит m элементов, поскольку выражается через m элементов системы субмодулей: $a_{m+1} = (a_{m+1,1}, a_{m+1,2}, ..., a_{m+1,m})$; $m + 2$-элемент содержит $2 \cdot m$ элементов, поскольку выражается через m элементов системы субмодулей и m элементов вектора a_{m+1}. Таким образом, продолжая рассуждения, можно заключить, что число элементов L_i для вектора a_i может быть выражено следующей формулой:

$$L_i = \begin{cases} 1, & i \le m \\ 2^{i-m-1} \cdot m, & m < i \le n \end{cases}. \quad (1)$$

Общее же число элементов L вектора A можно рассчитать, воспользовавшись формулой суммы геометрической прогрессии [6]:

$$L = \sum_{i=1}^{i \le n} Li = m + m \cdot (2^0 + 2^1 + \ldots + 2^{n-m-1}) = m \cdot \left(1 + \frac{2^{n-m} - 1}{2 - 1}\right) = 2^{n-m} \cdot m. \quad (2)$$

Рассмотрим численный пример. Пусть задана система модулей: $(p_1, p_2, p_3, p_4, p_5) = (2, 3, 5, 29, 863)$. $P = 2 \cdot 3 \cdot 5 \cdot 29 \cdot 863 = 750810$. Также необходимо убедиться, что $2 \cdot 3 > 5$, $2 \cdot 3 \cdot 5 > 29$, $2 \cdot 3 \cdot 5 \cdot 29 > 863$. Выберем систему базовых модулей (p_1, p_2). В этом случае $Q = p_1 \cdot p_2 = 6$, $n = 5$, $m = 2$. Число элементов вектора $L = 2^3 \cdot 2 = 16$.

Разложим число $A = 865$, заданное в позиционной системе счисления, в вектор по обычному базису:

$$A = \left(|865|_2,\ |865|_3,\ |865|_5,\ |865|_{29},\ |865|_{863}\right) = (1,\ 1,\ 0,\ 24,\ 2).$$

Теперь разложим число A по рекурсивному базису:

$$A = \Big(|865|_2,\ |865|_3,\ \big(\|865|_5|_2,\ \|865|_5|_3\big),$$
$$\big(\|865|_{29}|_2,\ \|865|_{29}|_3,\ \big(\|\|865|_{29}|_5|_2,\ \|\|865|_{29}|_5|_3\big)\big),$$
$$\big(\|865|_{863}|_2,\ \|865|_{863}|_3,\ \big(\|\|865|_{863}|_5|_2,\ \|\|865|_{863}|_5|_3\big),$$
$$\big(\|\|865|_{863}|_{29}|_2,\ \|\|865|_{863}|_{29}|_3,\ \big(\|\|\|865|_{863}|_{29}|_5|_2,\ \|\|\|865|_{863}|_{29}|_5|_3\big)\big)\big)\big) =$$
$$\Big(1{,}1,\ (0{,}0),\ \big(0{,}0,(0{,}1)\big),\big(0{,}2,\ (0{,}2),\ \big(0{,}2,\ (0{,}2)\big)\big)\Big).$$

Поскольку все числа в этом векторе не превышают 3, то для хранения вектора потребуется $16 \cdot 2 = 32$ бит, вместо 20 бит для хранения числа в позиционной системе счисления. Степень избыточности составит 1,6. Иллюстрацию к примеру см. на рис. 3.

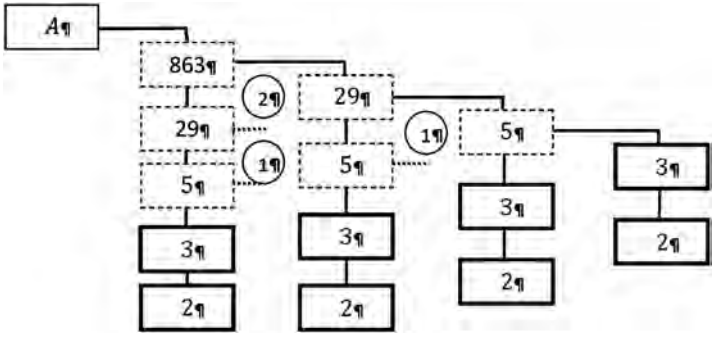


Рис. 3. Разложение числа в системе (2, 3, 5, 29, 863) через систему базовых модулей (2, 3)

3.2. Ограничения на выбор базиса

Максимальное значение, которое можно представить с помощью p_{m+1}, равно $\max = p_{m+1} - 1$. Чтобы была возможность выполнять арифметические операции над числами, требуется, чтобы результат операции для p_{m+1}-элемента был меньше $Q = (p_1 \cdot p_2 \cdot \ldots \cdot p_m)$. Для сложения это будет $2 \cdot \max$, а для умножения — $\max^2$.

Рассмотрим следующий пример. Пусть задан базис (2, 3, 5). Выберем систему базовых модулей как (2, 3). В этом случае $Q = 2 \cdot 3 = 6$, $\max = 4$. Поскольку для сложения потребуется максимально представимое число 8, что больше 6, а для умножения — 16, что тоже больше 6, то в таком базисе можно выполнять взаимно-однозначное разложение чисел, но для базовых арифметических операций он не подходит. Для реальных задач требуется увеличение числа Q.

Как именно выбирать элементы базиса? Рассмотрим следующий пример. Пусть задана система базовых модулей (4, 5, 7). Требуется определить p_4, чтобы в рамках такого рекурсивного базиса можно было использовать операцию умножения.

$$Q > MAX \rightarrow Q > \max^2 \rightarrow Q > (p_4 - 1)^2 \rightarrow p_4 < \sqrt{Q} +$$

$$+1 \rightarrow p_4 < \sqrt{140} + 1 \rightarrow p_4 < 12{,}8$$

Следовательно, для реализации рекурсивного базиса мы можем выбрать $p_4 = 11$.

3.3. Обратное преобразование числа из рекурсивного представления в позиционное

Для обратного представления также требуется рекурсивная реализация на базе того же метода, который используется для преобразования из вектора традиционной модулярной арифметики в позиционную систему счисления.

Пусть задан некоторый вектор $A = (a_1, a_2, \ldots, a_n)$. Из свойств систем остаточных классов известно, что

$$A = (a_1, a_2, \ldots, a_n) = (a_1, 0, \ldots, 0) + (0, a_2, \ldots, 0) + \ldots + (0, 0, \ldots, a_n) =$$

$$= \left| \sum_{i=1}^{n} a_i \cdot B_i \right|_P,$$

где $B_0 = (1, 0, \ldots, 0)$, $B_1 = (0, 1, \ldots, 0)$, $\ldots$, $B_n = (0, 0, \ldots, 1)$ — система ортогональных базисов [7].

В рекурсивной модулярной арифметике требуется найти набор ортогональных базисов для следующих систем остаточных классов:

$$(p_1, p_2, ..., p_m), (p_1, p_2, ..., p_{m+1}), ..., (p_1, p_2, ..., p_n).$$

Рассмотрим пример. Пусть задан базис (3, 5, 7, 11, 13) с системой базовых модулей (3, 5, 7) и пусть требуется преобразовать вектор (1,2,1, (0,3,3), (0,1,6, (0,1,6)) в позиционную систему счисления. Для обратного преобразования требуется найти ортогональные базисы для каждой из следующих систем остаточных классов:

$S_1 = (3, 5, 7) \rightarrow B_{1,1} = (1, 0, 0) \equiv 70; \quad B_{1,2} = (0, 1, 0) \equiv 21;$

$B_{1,3} = (0, 0, 1) \equiv 15;$

$S_2 = (3, 5, 7, 11) \rightarrow B_{2,1} \equiv 385; \quad B_{2,2} \equiv 231; \quad B_{2,3} \equiv 330; \quad B_{2,4} \equiv 210;$

$S_3 = (3, 5, 7, 11, 13) \rightarrow B_{3,1} \equiv 5005; \quad B_{3,2} \equiv 6006; \quad B_{3,3} \equiv 10725;$

$B_{3,4} \equiv 1365; \quad B_{3,5} \equiv 6930.$

Процесс обратного преобразования приведён на рис. 4. В позиционной системе счисления искомый вектор равен 13357.

Рис. 4. Процесс обратного преобразования вектора

3.4. Сложение и умножение в рекурсивной модулярной арифметике

Соответственно, если выполнены ограничения, наложенные на базис (см. раздел 3.2), то сложение и умножение чисел выполняется так же, как и в традиционной модулярной арифметике. Чтобы сложить (умножить) два числа, требуется сложить (умножить) соответствующие элементы вектора по модулю p_i. А поскольку все элементы вектора имеют малую разрядность, параллельное сложение (умножение) выполняется очень быстро.

4. Экспериментальные результаты

В рамках эксперимента сравнивалась скорость выполнения скалярного умножения векторов тремя способами: в позиционной системе счисления, в рамках обычного модулярного базиса и в рамках рекурсивного модулярного базиса.

Для построения модели устройств выбран маршрут проектирования цифровых ИС на основе библиотек стандартных ячеек. В маршруте используются: поведенческое описание устройства на языке Verilog HDL; средства логического синтеза Synopsys Design Compiler; средства статического временного анализа Synopsys Prime Time; библиотека стандартных ячеек Nangate Open Cell Library с проектными нормами 45 нм.

В разработанном устройстве для рекурсивной модулярной арифметики прямое преобразование выполняется конвейерным образом и задержка на прямое преобразование для заданных параметров всегда меньше, чем основное тело скалярного умножения. Обратное преобразование выполняется довольно долго, но из-за того что на обратное преобразование выделяется число циклов, равное числу элементов вектора, даже в самых сложных случаях обратное преобразование успевает завершиться намного раньше, чем на вход обратному преобразователю поступает новая порция данных.

Таким образом, тактовая частота устройства определяется блоком, имеющим максимальную задержку, а именно основным телом скалярного умножения.

Пусть вектора состоят из 1024 элементов, а аргументы у векторов 20-битные. Для этого потребуется вычислять сумму 1024 произведений, т. е. обеспечить $1024 \cdot \max^2 < 0$. Здесь не обойтись системой только трёхбитных базовых модулей. Добавим к ним четырёхбитные: 5, 7, 8, 9, 11 и 13 (Q = 360360). Для выбора ближайшего модуля воспользуемся формулами из раздела 4. Получаем $p_7 < 18$. Выбираем $p_7 < 17$. Аналогичным расчётом строим все дерево целиком: (5, 7, 8, 9, 11, 13, 17, 73, 659, 16963). Чтобы сделать такое устройство, нужно спроектировать блок из шести вычислителей (для каждого базового модуля), и таких блоков нужно будет 16. Вот где работает регулярность. Заметим, что все вычислители имеют крайне высокое быстродействие (суперраспараллеливание) и небольшие аппаратные затраты в силу малости значений базовых модулей.

Рассмотрим комбинационный участок синхронной схемы скалярного умножения (рис. 5).

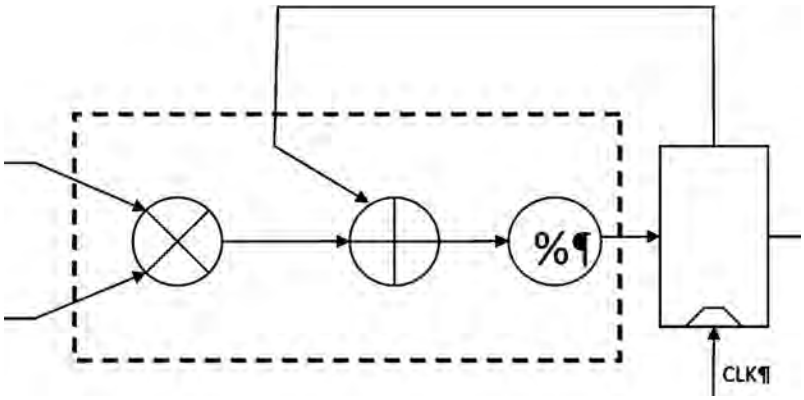


Рис. 5. Комбинационный участок скалярного умножения векторов

Устройство имеет тактовую частоту, которая напрямую зависит от длины критического пути на этом участке, и содержит три операции: умножение, сложение и взятие остатка по модулю.

Было разработано несколько потоковых устройств для скалярного умножения векторов. Каждое модулярное устройство состоит из трех участков: прямое преобразование из позиционной системы счисления, основной блок скалярного умножения

и обратное преобразование из рекурсивной модулярного представления в позиционное. Тактовая частота определяется самым медленным участком схемы. В нашем случае этим участком был блок скалярного умножения.

Оценивались максимальная тактовая частота и общая площадь устройства для трёх методов расчёта, обычная реализация в позиционной системе счисления, реализация в традиционной модулярной арифметике и реализация в рекурсивной модулярной арифметике. Результаты расчётов приведены в табл. 1, 2 и 3.

Таблица 1. Наборы модулей для скалярного умножения в традиционной и рекурсивной модулярной арифметике

Длина вектора	Разрядность данных (бит)	Набор модулей	
		модулярная арифметика	рекурсивная модулярная арифметика
512	16	7, 11, 13, 16, 17, 19, 23, 27, 29, 31	базовые: 5, 7, 8, 9, 13, 17 дополнительные: 31, 181, 709
1024	20	37, 41, 43, 47, 53, 59, 61, 63, 64	базовые: 5, 7, 8, 9, 11, 13 дополнительные: 17, 73, 659, 16963
2048	24	5, 7, 17, 31, 61, 67, 71, 73, 113, 127, 128	базовые: 13, 17, 19, 23, 29, 31 дополнительные: 199, 2903, 11497

Таблица 2. Тактовая частота разработанного блока для разных методов реализации

Длина вектора	Разрядность данных (бит)	Тактовая частота (МГц)		
		позиционная система счисления	модулярная арифметика	рекурсивная модулярная арифметика
512	16	409	726	855
1024	20	346	581	986
2048	24	294	537	794

Таблица 3. Площадь комбинационной части разработанного блока для разных методов реализации

Длина вектора	Разрядность данных (бит)	Площадь комбинационной части блока скалярного умножения		
		позиционная система счисления	модулярная арифметика	рекурсивная модулярная арифметика
512	16	3119	3928	11443
1024	20	5040	5857	22745
2048	24	6915	6742	26038

5. Недостатки рекурсивной модулярной арифметики и возможности для их нейтрализации

Основные недостатки предложенного метода:

1) аппаратная избыточность;
2) усложнение прямого и обратного преобразователей из позиционной системы счисления (усложняются также и другие немодульные операции);
3) ограничения на выбор базисов;
4) ограничение на количество последовательных операций без обращения к рекурсии.

Некоторые недостатки рекурсивной модулярной арифметики напрямую следуют из того факта, что маршрут включает в себя операцию нахождения вычета довольно больших чисел. В традиционной модулярной арифметике обычно используется только набор из малых модулей или модулей специального вида. В целях дальнейшего развития рекурсивной модулярной арифметики можно использовать в качестве модулей числа Мерсена [8] и/или числа вида $2^n \pm k$, для которых операция взятия остатка от деления на аппаратном уровне потребляет мало аппаратных ресурсов.

Литература

1. Устройство для вычисления по модулю // Патент на полезную модель № 103010. — Российская Федерация, МПК G06F7/72. заявитель ИППМ РАН. № 2010148522; заявл. 29.11.2010; зарег. 20.03.2011.

2. Акушский И. Я., Юдицкий Д. И. Машинная арифметика в остаточных классах. — М.: Сов. Радио, 1968. — 440 с.
3. Szabo N. S. and Tanaka R. I. Residue Number System and its applications to Computer Technology, McGraw-Hill, New York, 1967.
4. Soderstrand M. A. et al. (Eds), Residue Number System Arithmetic: Modern Applications in Digital Signal Proccessing, IEEE Press, NY, 1986.
5. Amos Omondi, Benjamin Premkumar. Residue Number Systems: Theory and Implementation, 2007.
6. Выгодский М. Я. Справочник по элементарной математике. — Москва, 2006.
7. Tseng B., Jullien G. A., Miller W. C. Implementation of FFT structures using the residue number systems. *IEEE Transactions on Computers*, 1992. 28(11).
8. http://ru.wikipedia.org/wiki/Числа_Мерсенна.

Опубликовано в журнале
«Информационные технологии»,
2013. — № 2. — С. 22–27.

Методы дополнительного сокрытия служебной информации в спутниковых каналах общего применения

Амербаев В. М., д. т. н., профессор, академик НАН РК
Любушкина И. Е., к. т. н., гл. специалист фирмы «АНКАД»

Введение

Ни одна автоматизированная информационная система не может существовать без передачи служебной информации. Именно служебная информация координирует работу и определяет настройки узлов системы. Одной из разновидностей автоматизированной информационной системы являются системы спутниковой связи.

В системах спутниковой связи, ориентированных на передачу пользовательской информации, под служебную инфор-

мацию, как правило, выделяется такой канальный ресурс, который позволит не сокращать объем и скорость передачи информации пользователей. Объем служебной информации оставляют минимально необходимым для поддержания работоспособности системы связи. Канальный ресурс, выделяемый под служебную информацию, принято называть каналом сигнализации. А канальный ресурс, выделяемый под пользовательскую информацию, как правило, образует совокупность абонентских каналов. При этом служебная и пользовательская информация передаётся в одном радиочастотном тракте, который доступен нарушителю. Существуют две проблемы, связанные с передачей служебной информации:

1) служебная информация должна быть надёжно защищена от раскрытия и подмены;
2) передача служебной информации должна быть надёжной. Повторная передача служебных пакетов нежелательна.

Предлагаемые методы позволяют решить обозначенные выше проблемы и повысить надёжность сокрытия и передачи служебной информации в каналах сигнализации системы спутниковой связи. Кратко рассмотрим эти методы.

Метод защиты от корреляционного прослушивания

Каналы сигнализации, организуемые в общем канальном ресурсе системы спутниковой связи, всегда доступны нарушителю для прослушивания и, следовательно, для изучения расписания, маршрутизации и интенсивности передач, а также содержимого передаваемой информации.

Проблемы сокрытия содержания передаваемых сообщений успешно решаются средствами защиты информации каналов сигнализации посредством преобразования алгоритма защиты информации, применяемого на информационном уровне взаимодействия. Но даже при использовании криптографических методов сокрытия содержания служебной информации при использовании одинакового ключа, синхропосылки и содержания пакета будет получаться одно и тоже значение на выходе криптографического алгоритма. В таком случае нарушитель, не зная содержания пакета, может отследить маршрут

информационных сообщений и проанализировать интенсивность и плотность передачи сообщений от передатчика на определённый приёмник. Организация подобного рода анализа приёмо-передающих трактов системы спутниковой связи реализуется следующим образом.

Нарушитель прослушивает и сохраняет весь поток информации пункта связи А и пункта связи Б. Он имеет возможность сравнить сохранённый информационный поток пункта связи А с информационным потоком пункта связи Б на предмет поиска одинаковых участков потока сообщений.

Таким образом, нарушителем определяется маршрутизация той части информационного потока, которая представляет для него повышенный интерес. Нарушитель может провести анализ периодичности, продолжительности и расписания передачи сигналов, а также корреляцию фактов передачи сообщений с социальными, экономическими и политическими событиями. Такой вид анализа работы системы связи был назван *корреляционным прослушиванием (или прослушиванием с сопоставлением).*

Противодействие корреляционному прослушиванию обеспечивается путём введения дополнительного преобразования информационного потока канала сигнализации, заключающегося в выработке псевдослучайной последовательности и её наложении по модулю два на кадровую структуру приёмо-передающего тракта.

Обеспечение преобразования декоррелирования каналов на БРК сводится к разработке алгоритма декоррелирования, удовлетворяющего следующим требованиям:

- алгоритм должен иметь гибкую программную реализацию, не привязанную к конкретной аппаратуре;
- алгоритм должен иметь гибкую схему покадровой синхронизации на приёмной и передающей стороне;
- входной параметр преобразования алгоритма должен быть долговременным;
- алгоритм должен иметь возможность преобразовывать информацию на проходе со скоростью выше скорости регенеративного преобразования информации на БРК

и вносить минимальные задержки в формирование кадра;

- быть вычислительно стойким (или условно стойким).

Наиболее подходящими для реализации в компьютерных системах процедур преобразования являются блочные шифры разового пользования, т. е. шифры, ключевой оператор которых явно зависит от временного параметра ***t***. Характер изменений этого параметра определяет временные интервалы «разового пользования» ключевым материалом.

Идея разового пользования была сформирована в явном виде в работе Р. Лидла и Г. Пильца «Прикладная абстрактная алгебра» на примере преобразования Л. Хилла, где рассматривается аффинное отображение Z_q^n на Z_q^n (здесь Z_q — кольцо вычетов по mod q кольца целых чисел Z):

$$y = K_t x + d, \qquad (1)$$

где элементы матрицы $\boldsymbol{K}_t$ зависят от временного параметра ***t***.

Для обратимости отображения (1) требуется, чтобы выполнялось условие

$$\text{НОД}\ (\det K_t, q) = 1. \qquad (2)$$

В такой постановке проблема разового пользования ключом сводится к задаче генерации квадратных матриц $\boldsymbol{K}_t$, зависящих от параметра ***t*** и удовлетворяющих условию (2).

Для ее решения были использованы инволютивные и треугольные матрицы. Естественно обобщить этот метод динамического (т. е. зависящего от ***t***) и биективного отображения Z_q^n на Z_q^n, базируясь на генерации в каждый момент ***t*** случайных матриц над Z_q требуемых порядков. Назовём этот метод обобщённым методом Хилла.

Сформируем сначала требования, предъявляемые к конструированию подобных отображений.

Первое требование: отображение должно удовлетворять принципу Хопфа.

В классической работе «Теория связи в цифровых системах» К. Шеннон разработал ряд приёмов построения кодирующих (и декодирующих) отображений, которые направлены

на осложнение криптоанализа. Это так называемые методы распыления и зашумления, которые далее были синтезированы им в метод перемешивания. К. Шеннон отмечает, что к хорошему перемешиванию приводят не коммутирующие между собой процедуры (на примере исследований Е. Хопфа), а методы, использующие операции разнотипных (т. е. несовместимых) алгебраических систем. Именно последние требования в настоящей работе названы принципом Хопфа.

Второе требование — компьютерная согласованность. Конструируемое отображение должно использовать типы и структуры данных, операции над которыми допускают реализацию в используемой вычислительной среде.

Третье требование — принцип гибкой динамичности. Конструируемое отображение должно обеспечивать в каждый момент времени ***t*** гибкое управление рандомизацией ключевого материала.

Известный в вычислительной практике метод Гаусса — Зейделя решения систем уравнений подсказывает следующий прием построения динамичного биективного отображения Z_q^n на Z_q^n, удовлетворяющего перечисленным требованиям.

1. Модуль q выбирается в виде $q = 2^N$, где N — длина регистров используемой вычислительной среды. Предполагается, что арифметический процессор обладает устройством умножения двух N-битных операндов с сохранением $2N$-битного результата.

2. Генерируется «материнская» случайная матрица над Z_{2^N} или в более простом и более гибком случае «псевдослучайная матрица» размерности $n'n$:

$$\begin{pmatrix} a_{11} & a_{12}\dots & a_{12} \\ a_{21} & a_{22}\dots & a_{2n} \\ \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{nn} \end{pmatrix},$$

n*N бит — размерность блока данных за один раунд маскирования (демаскирования).

3. Прямое отображение формируется в форме Гаусса — Зейделя:

$$\begin{cases} y_1 = \left| x_1 + \lambda a_{11} x_2 \oplus a_{12} x_3 \oplus \ldots\ldots\ldots\ldots\ldots \oplus a_{1,n-1} x_n \lambda_N \oplus a_{1n} \right|_2^N; \\ y_2 = \left| x_2 + \lambda a_{21} x_3 \oplus a_{22} x_4 \oplus \ldots\ldots\ldots\ldots\ldots \oplus a_{2,n-1} y_1 \lambda_N \oplus a_{2n} \right|_2^N; \\ y_3 = \left| x_3 + \lambda a_{31} x_4 \oplus a_{32} x_5 \oplus \ldots \oplus a_{3,n-2} y_1 \oplus a_{3,n-1} y_2 \lambda_N \oplus a_{3n} \right|_2^N; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y_n = \left| x_n + \lambda a_{n1} y_1 \oplus a_{n2} y_2 \oplus \ldots \quad \ldots \oplus a_{n,n-1} y_{n-1} \lambda_N \oplus a_{nn} \right|_2^N. \end{cases}$$

При этом обратное отображение имеет ту же форму Гаусса — Зейделя:

$$\begin{cases} x_n = \left| y_n - \lambda a_{n1} y_1 \oplus a_{n2} y_2 \oplus \ldots\ldots\ldots\ldots\ldots\ldots\ldots \oplus a_{n,n-1} y_{n-1} \lambda_N \oplus a_{nn} \right|_2^N; \\ x_{n-1} = \left| y_{n-1} - \lambda a_{n-1,1} x_n \oplus a_{n-1,2} y_1 \oplus \ldots\ldots\ldots\ldots\ldots \oplus a_{n-1,n-1} y_{n-2} \lambda_N \oplus a_{n-1,n} \right|_2^N; \\ x_{n-2} = \left| y_{n-2} - \lambda a_{n-2,1} x_{n-1} \oplus a_{n-2,2} x_n \oplus a_{n-2,3} y_1 \oplus \ldots \oplus a_{n-2,n-1} y_{n-3} \lambda_N \oplus a_{n-2,n} \right|_2^N; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_1 = \left| y_1 - \lambda a_{11} x_2 \oplus a_{12} x_3 \oplus \ldots\ldots\ldots\ldots\ldots\ldots\ldots \oplus a_{1,n-1} x_n \lambda_N \oplus a_{11} \right|_2^N. \end{cases}$$

Здесь используются следующие обозначения:

- $|\,.\,|_2^N$ — операция взятия вычета по $\bmod 2^N$;
- $\oplus$ — операция побитного xor;
- $|a+b|_2^N$, $|a-b|_2^N$ — операции сложения и умножения по $\bmod 2^N$;
- ab — операция арифметического умножения двух N-разрядных целых чисел с формированием $2N$-битного результата;
- $\lambda.\lambda_N$ — операция детерминированного перемешивания битов $2N$-битного слова с получением в результате N-битного слова по следующей схеме: из $2N$-битного слова выделяется (псевдослучайно) блок из N бит, которые побитно перемножаются по модулю два с оставшимися N-битами исходного $2N$-битного слова.

Все используемые здесь операции не перестановочные и максимально приближены к программной реализации.

Интерполяционная защита от воздействия имитационных помех многоканального ствола

Под термином «ствол» понимается широкополосный приёмопередающий тракт, образованный между бортовым ретранслятором и центральной станцией, в котором в общем сигнале следует информация от нескольких абонентских станций. Имитационной помехой называется такая помеха, которая имитирует полезный сигнал и излучается кратковременно, пытаясь подменить собой сигнал истинного абонента. При этом либо часть, либо всё информационное сообщение абонента может быть потеряно. В составе информационного сообщения абонента также передаётся служебная информация от абонентской станции. При потере полного сообщения абонент пересылает его вновь. При потере части сообщения возможность восстановить потерянную часть представляется перспективным решением, экономящим канальный ресурс, который тратится на повторение потерянных данных. Алгоритм преобразования и восстановления данных базируется на интерполяционных полиномах Лагранжа. Ниже представлен алгоритм восстановления одного символа (пакета) сообщения.

Исходные данные

1. Вычисления ведутся в поле десятичных чисел по модулю простого числа p.

2. Зададим узлы (или отсчеты) интерполяционного полинома:

$$x1, x2, x3, ..., xn.$$

3. Разобьем сообщение на символы. Символы должны попадать в кольцо вычетов модуля выбранного простого числа.

$$\alpha 1, \alpha 2, \alpha 3, ..., \alpha n, \text{ где } |\alpha_i|_p = \alpha_i$$

Степень полинома должна быть больше или совпадать с количеством символов.

4. Форма полинома —

$$f(x) = \sum_{i=1}^{n} \alpha_i Z_n^{(i)}, \text{ где}$$

$$Z_n^{(i)}(x)=\frac{(x-x_1)(x-x_2)\ldots\ldots(x-x_{i-1})(x-x_{i+1})\ldots\ldots(x-x_n)}{(x_i-x_1)(x_i-x_2)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_n)}.$$

Алгоритм кодирования сообщения

1. Имеем символы сообщения:

$$\alpha 1,\ \alpha 2,\ \alpha 3,\ \ldots\ \alpha n$$

и узлы полинома

$$x1,\ x2,\ x3,\ \ldots,\ xn.$$

Это конкретные числовые значения.

2. Зададим два избыточных узла полинома.

$$x_{n+1},\ x_{n+2}$$

3. Рассчитаем значение функции $Z_n^{(i)}(x)$.
4. В избыточных узлах составим таблицу коэффициентов.

	$x = x_{n+1}$	$x = x_{n+2}$
$Z_n^1(x)$	γ_n^1	δ_n^1
$Z_n^2(x)$	γ_n^2	δ_n^2
...	...	...
...	...	...
...	...	...
$Z_n^n(x)$	γ_n^n	δ_n^n

$$\gamma_n^i = |Z_n^1(x_{n+1})|_p, \quad \delta_n^i = |Z_n^1(x_{n+2})|_p,$$

γ_n^i, δ_n^i — числовые значения.

Если длина сообщения известна и неизменна, то такая таблица составляется заранее и хранится в ПЗУ.

5. Избыточные символы сообщения находятся следующим образом:

$$\Delta_{n+1}=\left|\sum_{i=1}^{n}\alpha_i\gamma_n^i\right|_p \quad \text{и} \quad \Delta_{n+2}=\left|\sum_{i=1}^{n}\alpha_i\delta_n^i\right|_p.$$

6. Получаем сообщение, которое передаётся в канал связи:

$$\alpha 1, \alpha 2, \alpha 3, \ldots \alpha n, \Delta_{n+1}, \Delta_{n+2}.$$

Алгоритм декодирования сообщения

1. Пусть i-й символ пришёл с ошибкой (или вообще пропал в канале связи). Запишем $\hat{\alpha}_i = (\alpha_i + \sigma_i)$ (1), где α_i — истинное значение символов, σ_i — ошибка.

2. Вычислим значения избыточных символов от полученного сообщения. Считаем, что табл. 1 известна на приёмной стороне:

$$\Delta'_{n+1} = \left| \sum_{i=1}^{n} \alpha_i \gamma_n^i \right|_p ,$$

$$\Delta'_{n+2} = \left| \sum_{i=1}^{n} \alpha_i \delta_n^i \right|_p .$$

3. Найдем синдром ошибки:

$$|\Delta_{n+1} - \Delta'_{n+1}| = \lambda_1,$$

$$|\Delta_{n+2} - \Delta'_{n+2}| = \lambda_2.$$

Если ошибки в сообщении нет, то $\lambda_1 = \lambda_2 = 0$.

Если ошибка в избыточных символах, то $\lambda_1 = 0$ $\lambda_2 \neq 0$ или $\lambda_1 \neq 0$ $\lambda_2 = 0$.

Если оба числа $\lambda_1 \neq 0$ и $\lambda_2 \neq 0$, то ошибка в сообщении.

4. Считаем, что ошибка только в одном символе сообщения, номер этого сообщения неизвестен.

5. Найдем величину ошибки:

$$\left| \frac{\lambda_1}{\lambda_2} \right| = \rho_i ,$$

$$\rho_i = \left| \frac{Z_n^i(x_{n+1})}{Z_n^i(x_{n+2})} \right|_p = \left| \frac{(x_{n+1} - x_1)(x_{n+1} - x_2)\ldots(x_{n+1} - x_n)}{(x_{n+2} - x_1)(x_{n+2} - x_2)\ldots(x_{n+2} - x_n)} \right|_p .$$

Так как *i* (место ошибки) нам неизвестно, умножаем и делим получившееся сообщение на следующую дробь:

$$\frac{(x_{n+1}-x_i)}{(x_{n+2}-x_i)}.$$

Тогда получим следующее уравнение:

$$\rho_i = \left| \frac{P_n(x_{n+1})}{P_n(x_{n+2})} \cdot \frac{(x_{n+2}-x_i)}{(x_{n+1}-x_i)} \right|_p,$$

где $P_n(x) = (x-x_1)(x-x_2)...(x-x_n)$.

Рассчитаем значение дроби

$$L = \left| \frac{P_n(x_{n+1})}{P_n(x_{n+2})} \right|_p.$$

Далее производим расчеты:

$$\left| \rho_i \cdot L^{-1} \right|_p = \left| \frac{(x_{n+2}-x_i)}{(x_{n+1}-x_i)} \right|_p.$$

Обозначим $\rho_i \cdot L^{-1}$ как r_i, тогда

$$|x_{n+2}-x_i|_p = |r_i(x_{n+1}-x_i)|_p,$$

$$|x_i(r_i-1)|_p = |r_i x_{n+1} - x_{n+2}|_p,$$

$$x_i = \left| \frac{r_i x_{n+2} - x_{n+2}}{r_{i-1}} \right|_p.$$

Зная значение x_i, определим положение ошибки.

6. Рассмотрим уравнение

$$\left| \Delta_{n+1} - \Delta'_{n+1} \right| = \lambda_1.$$

Подставим в него значения

$$\Delta_{n+1} = \left| \sum_{i=1}^{n} \alpha_i \gamma_n^i \right|_p,$$

$$\Delta'_{n+1} = \left| \sum_{i=1}^{n} \hat{a}_i \gamma_n^i \right|_p.$$

Получим

$$\left| \alpha_i \gamma_n^i - \hat{a}_i \gamma_n^i \right|_p = \lambda_i. \qquad (2)$$

С учетом уравнения (1) и (2) получим

$$\left|-\sigma_i \gamma_n^i\right|_p = \lambda_1. \qquad (3)$$

Зная номер ошибочного сообщения, определенного из позиции x_i в системе узлов интерполяционного полинома, подставим соответствующий ему коэффициент в уравнение (3):

$$\sigma_i = \left|-\frac{\lambda_i}{\gamma_n^i}\right|_p.$$

7. Находим утерянный символ

$$\alpha_i = \left|\hat{a}_i - \sigma_i\right|_p.$$

Вывод

Представленные методы успешно решают проблему дополнительного сокрытия содержимого пакетов служебной информации, а также помогают обеспечить восстановление всего сообщения при утере одного пакета, чтобы исключить необходимость их повторов.

Публикуется впервые

Собственная безопасность информационных криптошифраторов и методы её реализации

Амербаев В. М., Зверев Е. М.,
Куцепалов Н. О., Любушкина И. Е.

Данная статья должна была появиться ещё при жизни Вильжана Мавлютиновича. Но этого не случилось. При подготовке данного сборника, посвящённого В. М. Амербаеву, его соавторы предложили включить в него статью.

Статья посвящена актуальному моменту, а в настоящее время это особо значимо, — вопросу повышения защищённости средств цифровой обработки информации и её передачи по различным каналам связи, управления и хранения в памяти.

В ней представлены методы и технические решения, обеспечивающие высокие информационно-защитные свойства

вновь создаваемой аппаратуры шифрования и, соответственно, обеспечения более высокой (определённо гарантированной) информационной безопасности данных, которые проходят через эту аппаратуру.

Статья аккумулирует технические решения, ранее опубликованные в различных ограниченно открытых источниках, но без описания в части практического их применения. Особо важным аспектом в статье представляются инновационно-идеологические методы надёжной некомпрометируемой микропроцессорной криптообработки шифруемых данных.

Объектом описания (в качестве примера) является широко представленный, многократно применённый в различных системах информационной защиты алгоритм СКЗИ (средство криптографической защиты информации) в соответствии с ГОСТ 28147-89. Этот стандарт являлся государственным алгоритмом криптографического преобразования в основном для несекретной, но ограниченного распространения информации (хотя при необходимости при выполнении дополнительных требований мог применяться и для секретной) в системах обработки и передачи цифровых данных и речи в телекоммуникациях, сетях ЭВМ, отдельных вычислительных комплексах, а также в средствах низовой и космической связи гражданского и военного назначения. Однако следует отметить, что на данный момент времени этот стандарт как самостоятельный не применяется, а входит в ранге режима «Магма» (определение ФСБ) в новый отечественный стандарт РФ ГОСТ Р 34.12. Но, когда велись работы и писалась статья, он действовал как самостоятельный стандарт. Поэтому далее будут рассматриваться функции защиты информации как элементы алгоритма шифрования с его старым названием. Тем более что его алгоритмические функции в составе режима «Магма» не изменены, кроме статуса таблиц замен (в новом ГОСТе таблица замен фиксированна и никоим образом не влияет на суть описываемой идеологии криптографических реализаций).

Он (стандарт) характеризуется высоким уровнем гибкого управления ключевыми параметрами шифрования, благодаря чему его криптографическая стойкость шифрования при определённых условиях не налагает ограничений на степень секретности защищаемой информации. ГОСТ 28147-89 обладает хорошими логико-техническими возможностями

в программной, аппаратной и в программно-аппаратной реализациях, благодаря чему завоевал широкую популярность у заказчиков и пользователей в различных областях применения. Он служит качественным средством защиты информационных процессов от несанкционированных и вредоносных воздействий на них, включая и защищаемую информацию.

В то же время представленная идеология обеспечения собственной информационной безопасности шифртехники в соответствии с ГОСТ 28147-89 для СКЗИ может быть распространена на любой тип криптошифраторов и, тем самым, значительно усиливать качественные характеристики последних.

Авторы

Стандарт шифрования СКЗИ ГОСТ 28147-89 [1] верно служит Отечеству уже более четверти века. Качество службы ГОСТ 28147-89 напрямую зависит от его собственной информационной безопасности, то есть способности противостоять информационно-физическим атакам со стороны информационных нарушителей и злостных её захватчиков.

Качество практической реализации средства криптографической защиты — СКЗИ, выполняющего криптопреобразования по ГОСТ 28147-89, определяет криптографическую надёжность (криптографическую стойкость) защиты информации в системе её обработки и/или связи. При этом криптографическая стойкость предопределяется способностью противостоять нарушителю в соответствии с моделью и классом защиты его целевой информации. То есть СКЗИ должно быть нечувствительно к неявным (невидимым, нерегистрируемым) атакам конкретного или потенциального нарушителя, пытающегося завладеть криптографически значимой информацией. СКЗИ не должно иметь уязвимости в системе защиты информации, а также возможности создавать механизмы как пассивного, так и активного доступа к защищаемой информации [2, 3, 4, 6, 8].

Соответственно, системная криптографическая надёжность (криптографическая стойкость) изделия СКЗИ, реализующего алгоритм защиты информации по ГОСТ 28147-89, определяется:

1) условиями применения и адекватностью принятой модели нарушителя;
2) физической живучестью СКЗИ и платформы/среды, в которую они встраиваются;
3) противодействием и блокированием возможностей несанкционированного встраивания в СКЗИ деструктивных аппаратных и/или программных элементов;
4) качеством исполнительного ключа шифрования и его защиты;
5) качеством вычислительного процесса при выполнении алгоритма шифрования;
6) качеством нелинейного узла замены;
7) контролепригодностью алгоритма, СКЗИ и среды, в которую они встраиваются;
8) качеством реализации средств противокомпрометационной защиты СКЗИ и среды, в которую они встраиваются.

Первые три позиции обеспечения криптографической надёжности присущи, как правило, любой криптографической системе и применимы в том числе и для СКЗИ на основе ГОСТ 28147-89. Они многократно представлены во множестве научных и технических описаний криптографических реализаций средств защиты информации [2, 5, 6], и для данной статьи они не представляют особого интереса.

Для СКЗИ на основе ГОСТ 28147-89 интересно рассмотреть вопросы обеспечения криптографической надёжности в соответствии с позициями 4–7. Все позиции направлены на блокирование проявлений криптографически опасной информации и соответствующих деструктивных атак на них в побочных каналах СКЗИ и среды, в которую последние встраиваются. Побочные каналы (на инженерном жаргоне — «побочки») это так называемые ПЭМИН — побочные электромагнитные излучения, наводки и пульсации в цепях питания, несущие в себе информационные сигналы или «следы» обработки криптографически опасной информации — КОИ. К КОИ рекомендуется относить открытую засекречиваемую/защищаемую информацию, ключи шифрования, аутентифицирующую и парольную

информацию, промежуточные гаммы формирования шифра (по методическим рекомендациям 8-го центра ФСБ России от 21.02.2008 г. № 149/54-144 «Криптографически опасная информация (КОИ) — информация о состояниях криптосредства, знание которой нарушителем позволит ему строить алгоритмы определения ключевой информации (или её части) или алгоритмы бесключевого чтения») [4, 8].

Комплекс организационно-технических мероприятий и средств, ориентированных на противокомпрометационную защиту КОИ в ПЭМИН, относится к тематике специальной защиты [4, 8]. ПЭМИН в открытой печати широко стали исследоваться с 80-х годов прошлого века [29–34]. Особенно активно эти исследования проводятся на несимметричных шифраторах как более доступных.

Расширенное понятие КОИ, сопутствующее процессам создания и использования защищаемых данных, может быть представлено следующим перечнем:

- ключевая, аутентифицирующая и парольная информация криптосредства;
- структурно-конфигурационная информация криптосредства;
- отдельные функциональные элементы криптографического алгоритма (например нелинейные узлы замены);
- режимные элементы функционирования криптографического алгоритма и/или его частей;
- управляющая информация СКЗИ и среды их встраивания;
- информация, регистрируемая в электронных журналах;
- побочные сигналы, которые возникают в процессе функционирования технических средств и в которых полностью или частично отражаются защищаемые данные или другая чувствительная к компрометации информация.

Возможными каналами атак, в частности, могут быть:

- каналы непосредственного доступа к объекту атаки (СКЗИ, их электронные и электрофизические элементы

и интерфейсные связи, а также той среды, в которой размещены СКЗИ);
- носители информации (например ключей);
- носители информации, выведенные из употребления;
- технические каналы утечки (в том числе проходящие вблизи СКЗИ);
- сигнальные цепи;
- цепи электропитания;
- цепи заземления;
- каналы утечки за счёт электронных устройств негласного получения информации (от внедрённых «закладных» устройств, и/или вредоносных программных фрагментов, и/или внешнего частотного облучения);
- информационные и управляющие интерфейсы;
- резервные копии файлов с защищаемой информацией, которые могут создаваться в процессе обработки этих файлов;
- остаточная КОИ на носителях информации.

Наибольшая опасность от ПЭМИН возникает в режиме подготовки и обработки защищаемых данных.

В данной статье предполагается рассмотреть пассивные атаки, которые практически не влияют на работу изделия, а также активные атаки (всевозможные виды радиоэлектронного облучения), которые также не нарушают режимы работы изделия.

Атаки и их последствия, связанные с проникновение внутрь изделия, как правило, защищены средствами от несанкционированного доступа (НСД), и мы их не рассматриваем [2, 7].

Пассивные атаки заметить и предотвратить практически невозможно. Они более выгодны для нарушителя с экономической точки зрения, т. к. атаки почти не требуют увеличения стоимости оборудования для их проведения [2, 7]. Именно пассивные атаки в первую очередь представляют собой угрозу неявной (скрытой) компрометации СКЗИ.

Использование мер и средств снижения информационно-компрометирующей составляющей в побочных сигналах и наводках требует дополнительного аппаратно-временного ресурса СКЗИ-изделия.

Основные методы и средства защиты от вредоносных атак:

1) защита от вредоносных (деструктивных) элементов аппаратных и программных закладок;
2) обеспечение качества схемных и программных решений, а также важный момент — монокристальность обработки КОИ;
3) многоразрядная параллельная обработка и параллельное зашумление;
4) обратные/равновесно электрические нормализующие коды данных и адресации КОИ;
5) временная нормализация;
6) разделение времени выполнения вычислительных процессов;
7) создание временной недетерминированности вычислительного процесса;
8) применение несовпадающих ключей доставки и ключей хранения;
9) применение динамической маски хранения и маски вычисления;
10) защита узла замены;
11) контролепригодность;
12) системно-корректное встраивание СКЗИ в среду взаимодействия.

Алгоритмические методы защиты ГОСТ 28147-89 от компрометации и обеспечение криптографической надёжности должны рассматриваться при безусловном выполнении п. 2 вышеприведённого перечня противокомпрометационных мер. Эти меры (п. 2) предполагают применение для разработки и производства СКЗИ высокоинтегрированной элементной базы — микропроцессоров и программно-логических монокристальных (для библиотечных элементов) отечественных БИС/ПЛИС (ПЛИС 5578ТС084 и 5578ТС094), адекватных, но не равных матрицам Altera, FPGA, Xilinx и др. Последние в определенных случаях при выполнении специальных дополнительных требований также могут применяться для реализации криптонадёжных шифраторов. В высокоинтегрированном

кристалле каждый базовый логико-схемотехнический элемент (триггер, инвертор и другие электронные составляющие) выполняется в едином технологическом процессе. Соответственно, электрофизические переключательные параметры однотипных элементов будут иметь минимальный разброс друг от друга. Последнее чрезвычайно важно для качественной реализации требований, предъявляемых к создаваемым СКЗИ. Эти свойства являются основополагающими в построении вычислительных процессов криптографических преобразований и обработки КОИ. Важным аспектом применения высокоинтегрированной элементной базы является ещё и то, что все электрофизические межблочные связи получаются минимальными, а соответственно, становятся и минимальными информационно-сигнальные пересылки по ним. Последние определяют минимальное электромагнитное излучение и наводки на внешнюю среду [3], что хорошо коррелируется с требованиями, предъявляемыми к СКЗИ.

Создание средств криптографической техники не допускает небрежного проектирования схемотехнических плат, модулей, блоков, устройств. Для этой техники не допускается невыполнение требований, определяющих качество защиты информации.

1. Качество схемотехнических и конструкторских решений заключается в корректной разводке шин питания и земляных шин по принципу «звезды» или «дерева». Не рекомендуется допускать шлейфовое проведение цепей питания и/или их «закольцовывание». Например, если имеются речепреобразующее устройство и устройство СКЗИ как отдельные электронные блоки, то их шины питания не должны иметь шлейфового межблочного соединения, а должны выходить на общую линию от блока питания через одни точки контактирования. Сигнальные межблочные линии должны быть экранированы. Модульные слои печатных плат желательно разделять экранными слоями. Входные, выходные цепи портов, разнесённых блоков (модулей) должны иметь качественно рассчитанные фильтры. Сами СКЗИ, точнее блоки/модули, работающие

с КОИ, желательно закрывать экраном. В настоящее время в зарубежных источниках описываются рекомендации реализации систем защиты информации с функционально-блочным разделением на «окрашенные» подсистемы «красные» — «синие» — «черные» [9, 10]. Где «красные» — это подсистемы, обрабатывающие открытую информацию; «синие» — выполняющие криптообработку и работающие с ключами; «черные» — не имеющие дела с КОИ, а работающие с несекретной и/или зашифрованной информацией. В отечественных описаниях это так называемые грязные и чистые функционалы. Где «грязные» — это то же самое, что «красные» и «синие» подсистемы, обозначенные в предыдущем случае, а «чистые» соответствуют «черным» подсистемам. И в первом, и во втором случаях подобное распределение с точки зрения качественной реализации системы информационной защиты является целесообразным.

На качество аппаратной платформы серьёзное влияние оказывает элементно-узловая база, а точнее — их комплектация. Так как разработка аппаратных функционалов сегодня производится в большей части на элементной базе зарубежного производства, то, соответственно, не гарантируется их чистота от возможных аппаратных деструктивных закладных элементов. Поэтому обязательным условием качества аппаратуры является проведение специальных проверок в специализированных организациях. Последние выдают соответствующее заключение на отсутствие деструктивных вложений. Проверкам подвергаются либо 100% элементной базы, либо выборочно из поставляемой партии от одной фирмы-поставщика. Введение «закладных» элементов — это политика отдельных государств, заинтересованных в контроле стратегически важной информации так называемых «партнёров» и потенциальных противников. Поэтому в этом плане целесообразны закупки элементной базы у разных фирм — производителей одноименных элементов.

2. Качество программных решений, создаваемых СКЗИ, как и в предыдущем пункте, имеет наиважнейшее значение.

Во-первых, ПО СКЗИ и ПО среды, в которой оно работает, должны быть защищены от возможности установки в них любых деструктивных программных (разрушающих, подслушивающих, копирующих и любых других подобного типа) закладок и вирусоподобных программ.

Во-вторых, в рабочих программах должны отсутствовать все отладочно-технологические входы/выходы, исключающие возможности создания так называемых люков для проникновения нарушителя в программную среду обработки и хранения КОИ в целях проведения программно-деструктивных атак на СКЗИ. ПО СКЗИ должно быть выполнено в соответствии с требованиями разработки надёжных программных продуктов [11] и рекомендаций, представленных в [12–13]. ПО СКЗИ должно представлять собой доверенную контролируемую и самоблокирующую программно изолированную среду [14, 15, 16]. Самоблокирующая программная среда — программная среда, позволяющая осуществлять блокировку недекларированных деструктивно-алгоритмических возможностей, которые потенциально могли бы присутствовать в заимствованных программных модулях. Если возникает крайняя необходимость использования покупного ПО, не обеспеченного исходными кодами, то должна использоваться технология создания ПО с применением так называемых белых — доверенных и чёрных — недоверенных программных модулей [16]. Первые должны исключать возможность заимствованному «чёрному» ПО (не сертифицированному по требованиям информационной безопасности) быть инициативным при обработке данных, команд и каких-либо обменов. То есть все действия привлечённого ПО должны быть подконтрольны основному управляющему криптоядру СКЗИ. Всё ПО — и основное, и вспомогательное, СКЗИ и программной среды, в которую оно погружено, должно быть имитозащищено с возможностью его тестирования как от собственного внутреннего контролирующего ключа, так и от внешнего специального ключа, вводимого от элементов управления либо из внешнего канала.

Положительным качеством блочного СКЗИ по ГОСТ 28147-89 является то, что обработка КОИ в нём ведётся в широкоформатном представлении данных (32 параллельных бита). То, что широкоформатная параллельная обработка существенно ускоряет вычислительный процесс шифрования информации, является существенным, но не определяющим фактором. Более существенным является то, что широкоформатная параллельная обработка повышает качество противокомпрометационной защиты КОИ. Точнее, снижается его информационная составляющая в побочных каналах ПЭМИН. Это связано с тем, что криптографически значимая цифровая информация в двоичном представлении имеет близкое к равномерному (равновероятному) распределение числа битов в слове обработки, то есть с незначительным преобладанием одних двоичных битов над другими. В соответствии с требованиями, предъявляемыми к СКЗИ, это так называемое преобладание Δ, которое может исчисляться от долей до единиц процентов. Это означает, что суммарная информационно-энергетическая переключающая составляющая электронных элементов в вычислительном процессе СКЗИ для любого криптографически информационного бита будет минимальна [17]. А именно: переключательный информационно-энергетический момент в линейке параллельных битов (в рамках разрядной сетки вычислителя) для всех обрабатываемых данных — КОИ будет нормализованным и теоретически равным. Соответственно, криптоаналитик, работающий с «побочкой», не имеет возможности выделить для анализа необходимый объем информации, компрометирующей шифр или его составляющие — КОИ. Ему остаётся работать с информацией, соответствующей предельно малым долям процентов Δ. Этот процент может быть уменьшен практически до нулевого значения Δ, и это является актуальным. Средством такого решения является когерентное электромагнитное зашумление работающего целевого шифратора излучением, создаваемым синхронно работающим с ним дублирующим шифратором, который бы обрабатывал также целевую информацию, но представленную противофазными

кодами (в информационном и логическом смысле), так называемыми равновесными кодами — РКД [17]. При этом суммарная переключательная информационно-энергетическая составляющая шума от обоих элементов обработки приближается к нулю. Данный факт был исследован в НИИ автоматики еще в 80-х годах. Однако применение его было невозможно, т. к. отсутствовала соответствующая элементная база у нас и за рубежом. Применение РКД для реализации СКЗИ как элемента вычислительного процесса для алгоритма ГОСТ 28147-89 стало возможным только с появлением высокоинтегрированной элементной базы БИС. Например, в его программной реализации кодовое равновесие может быть достигнуто, если каждое слово КОИ будет дополнено его обратным (электрически и логически противофазным) значением. При этом обработка будет выполняться синхронно (при условии реализации логических элементов в монокристальной структуре матрицы БИС/ПЛИС) как над прямым кодом, так и над его обратным значением. То есть всегда в обработке будет участвовать суммарно равное число битов единиц и нулей. В этом случае информационное Δ-преобладание (одних над другими) будет нулевым.

Эффективной является реализация алгоритма в специализированной двухпроцессорной вычислительной архитектуре БИС типа «Блюминг» [28]. В подобной архитектуре каждый процессор выполняется по адекватной архитектуре (см. рис. 1), например, с её расширением для синхронной параллельной работы в однокристальной системе. Адекватность выполнения арифметических операций алгоритма ГОСТ 28147-89 в РКД и их семантическая равнозначность поясняются ниже.

Криптосхема СКЗИ по ГОСТ 28147-89 (рис. 1) имеет сумматоры СМ1 и СМ3 по модулю 2^{32}, СМ4 по модулю 2^{32}—1, СМ2 и СМ5 модулю 2 [1].

Покажем, что все сумматоры имеют семантическую равнозначность для равновесных (противофазных) кодов.

Выразим работу двоичных сумматоров СМ1 и СМ3 криптосхемы ГОСТ 28147-89, представленной на рис. 1, в противофазных кодах операндов.

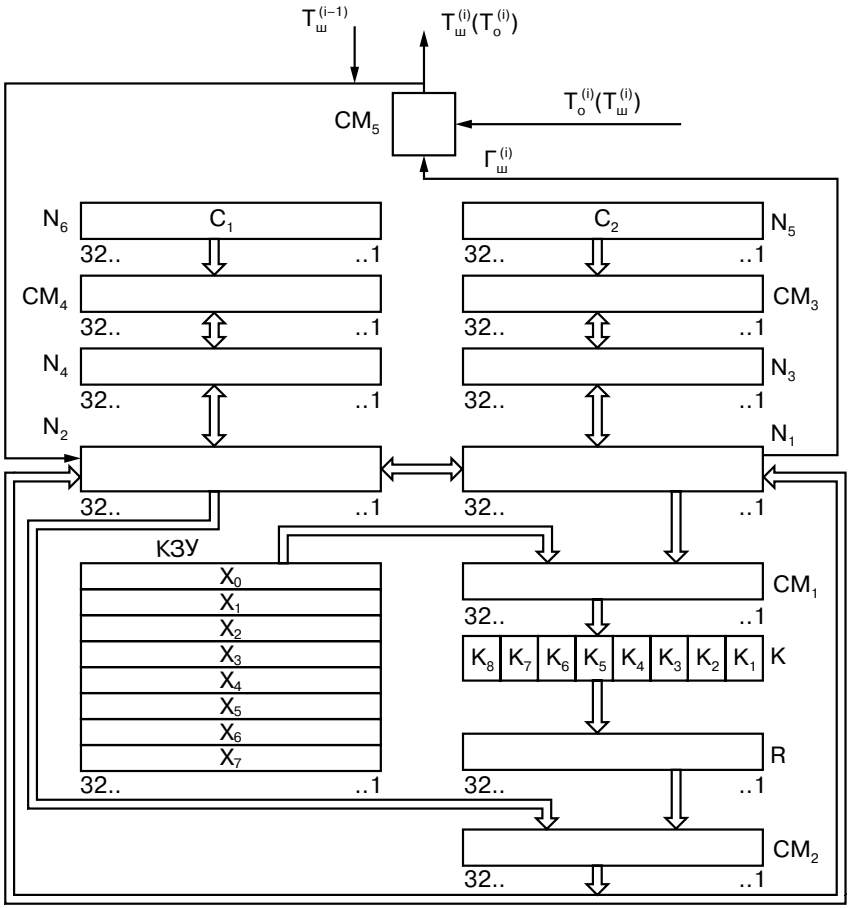


Рис. 1. Криптосхема СКЗИ по ГОСТ 28147-89

С этой целью заметим, что для подавления информации в шумах при работе с таблицами замены достаточно иметь параллельно действующий шифратор с таблицами замен, работающими в кодовой противофазе. То есть если на основном шифраторе в данный момент данного раунда «обрабатывается» информационный n-битный объект a, то в тот же момент на шифраторе, генерирующем «антикоды», должен обрабатываться противофазный информационный объект $\overline{a}$, такой, что $a+\overline{a}=2^n-1$.

Остановимся на том, как должен работать n-битный сумматор в противофазе, то есть в равновесном коде [17]. С этой целью введём ряд понятий и обозначений из теории сравнений — раздела теории чисел.

Символом Z_2n обозначим кольцо всех остатков (называемых также вычетами по mod 2^n), полученных от деления целых чисел на число 2^n. Множество Z_2n состоит из целых чисел: $0 \le a < 2^n$. Очевидно, что числа этого множества единственным образом изображаются двоичным кодом длины n, Z_2n является кольцом. Ниже достаточно рассмотреть аддитивную итерацию этого кольца:

$$\forall a,b \in Z_{2^n},$$

$$a \boxplus b := |a+b|_{2^n},$$

где правая часть представляет собой двоичное число, равное остатку от деления двоичной суммы чисел a и b на 2^n.

Остаток от деления произвольного целого числа $x \in Z$ на 2^n обозначим символом $|x|_{2^n}$.

Таким образом, теорема деления Евклида целых чисел [18] для данного случая будет выглядеть следующим образом:

$$\forall x \in Z, \qquad x = q \cdot 2^n + |x|_{2^n}.$$

Здесь q называется неполным частным от деления x на 2^n, его принято обозначать символом

$$q := \left[\frac{x}{2^n}\right].$$

Соответственно, величина $|x|_{2^n}$ называется остатком от деления x на 2^n.

Важными свойствами, использованными ниже, являются:

$$\forall x \in Z_{2^n} \qquad |x|_{2^n} = x, \tag{1}$$

$$\forall x,y \in Z \qquad |x+y|_{2^n} = \left||x|_{2^n} + |y|_{2^n}\right|_{2^n}, \tag{2}$$

$$\forall x \in Z_{2^n} \qquad \bar{x} := 2^n - 1 - x.$$

Очевидно, $\bar{x} \in Z_{2^n}$ и $\forall x \in Z_{2^n}$

$$x + \bar{x} = 2^n - 1. \tag{3}$$

Если $a \in Z_{2^n}$, то элементом, находящимся в противофазе, будем называть элемент $\bar{a}$, такой, что:

$$\bar{a} := 2^n - 1 - a.$$

Задача

Требуется разработать сумматор $\bar{\Sigma}_{2^n}$, работающий в противофазе с сумматором Σ_{2^n}. Точнее, если прямой сумматор реализует операции $|a+b|_{2^n}$, то сумматор, работающий в противофазе, реализует следующую операцию: на вход подаются операнды $\bar{a}$, $\bar{b}$, а на выходе получится результат $\overline{|a+b|}_{2^n}$.

Решение

Пусть $a, b \in Z_{2^n}$.

В силу (3)

$$\overline{|a+b|}_{2^n} = 2^n - 1 - |a+b|_{2^n}. \tag{4}$$

Согласно теореме деления Евклида

$$\overline{|a+b|}_{2^n} = a + b - \xi_0 \cdot 2^n,$$

где $\xi_0 = \left[\frac{a+b}{2^n}\right]$.

Подставим последнее тождество в (4), получим

$$\overline{|a+b|}_{2^n} = 2^n - 1 - (a+b) + \xi_0 \cdot 2^n. \tag{5}$$

Далее воспользуемся тождеством (3) и правую часть тождества (5) приведем к виду

$$\overline{|a+b|}_{2^n} = \bar{a} + \bar{b} + \xi_0 2^n - 2^n + 1.$$

Найдём остаток от деления последнего тождества (слева и справа) на 2^n. Тогда получим

$$\left|\overline{|a+b|}_{2^n}\right|_{2^n} = \left|\bar{a} + \bar{b} + 1\right|_{2^n}.$$

Но так как

$$\overline{|a+b|}_{2^n} \in Z_{2^n},$$

то согласно (1)

$$\left|\overline{|a+b|_{2^n}}\right|_{2^n} = \overline{|a+b|_{2^n}}.$$

Итак, получено тождество

$$|\bar{a}+\bar{b}+1|_{2^n} = \overline{|a+b|_{2^n}}, \qquad (6),$$

с помощью которого решается поставленная задача:

$$\Sigma_{2^n} + 1 (\mathrm{mod}\, 2^n) \to \overline{|a+b|_2}.$$

То есть инверсный (равновесный) сумматор по $\mathrm{mod}\, 2^n$ должен иметь на входе суммирования, помимо аргументов $\bar{a}$ и $\bar{b}$, еще аргумент в виде константы, равной 1, в младшем разряде сумматора.

Далее рассмотрим логику сумматора СМ4 по модулю $2^{32}-1$:

a — исходный код,

$\bar{a}$ — противофазный код исходному a, тогда

$$a + \bar{a} := 2^n - 1. \qquad (7).$$

Пусть даны два операнда

$$a, b \in Z_{2^n}.$$

Требуется найти противофазный код суммы $|a+b|_{2^n-1}$.

Согласно (7)

$$a + b = 2(2^n - 1) - (\bar{a} + \bar{b})$$

или

$$|a+b|_{2^n-1} = |-(\bar{a}+\bar{b})|_{2^n-1}.$$

Но $|-(\bar{a}+\bar{b})|_{2^n-1} = \left|2^n - 1 - |\bar{a}+\bar{b}|_{2^n-1}\right|_{2^n-1}$.

Следовательно,

$$\overline{|a+b|}_{2^n-1} = |\bar{a}+\bar{b}|_{2^n-1}.$$

Это означает, что в шифраторе перестраивать сумматор Σ_{2^n-1} не следует. Так, если на его входы подаются противофазные коды $\bar{a}$ и $\bar{b}$, то сумматор Σ_{2^n-1} выдаст на выходе код суммы $\overline{|a+b|}_{2^n-1}$ в противофазе, что и требовалось получить (!).

Рассмотрим логику сумматора СМ2 и СМ5 по модулю 2 на основе табличного представления [20].

a	b	$a \oplus b$	$\bar{a}$	$\bar{b}$	$\bar{a} \oplus \bar{b}$
a	0	a	$\bar{a}$	1	a
0	b	b	1	$\bar{b}$	b
a	1	$\bar{a}$	$\bar{a}$	0	$\bar{a}$
1	b	$\bar{b}$	0	$\bar{b}$	$\bar{b}$

Из таблицы видно, что результаты сложения по модулю 2 данных прямого и обратного представления равны.

То есть

$$\bar{\bar{a}} \oplus \bar{\bar{b}} = a \oplus b = \bar{a} \oplus \bar{b}.$$

Если представить

$$\bar{a} \oplus \bar{b} = x, \text{ а } x \oplus 1 = \bar{x}, \text{ то } a \oplus b \oplus 1 = \overline{\bar{a} + \bar{b}}.$$

Из последнего видно, что взаимно противофазное представление результатов по модулю 2 сумматоров может быть получено либо инвертированием результата с выхода сумматора (менее желательное решение), либо, если сумматор оканчивается регистровой схемой, возможен съём данных с его инверсного плеча триггерных схем.

Общие соображения, представленные выше, показывают, что актуальная техническая проблема построения дублирующего шифратора, работающего параллельно и в противофазе основному шифратору (в целях подавления компрометирующей информации в ПЭМИН), корректна и допускает техническое решение.

Данное техническое решение отмоделировано и практически реализовано авторами статьи, что показало его высокую эффективность в изделии заказчика.

Частичной (как полумера) противокомпрометационной защитой является реализация СКЗИ ГОСТ 28147-89 в широкоформатном исполнении, например, когда на микропроцессоре (типа фирмы TI) с 48-разрядным вычислительным АЛУ полноформатные равновесно-кодовые процедуры не проходят, если обработка целевых данных производится по 32 бита. В этом

случае элемент противокомпрометационной защиты можно улучшить посредством заполнения оставшихся 16 бит 48-битного регистра данными ГСЧ, которые как бы участвуют (псевдоучаствуют) в криптообработке. При этом Δ-преобладание на целевых данных снижается за счёт распределения его на все 48 разрядов вычислителя, уменьшая тем самым возможности криптоанализа от ПЭМИН [18]. Но это один из вариантов.

Равновесно-кодовую обработку целесообразно применять на всех ветвях алгоритма, включая адресно-табличные преобразования. Например, работа с узлами замены — в этом применении РКД для криптоаналитика в ПЭМИН начисто скрывает нелинейные криптопреобразования и их составные части.

Равновесно-кодовую технологию обработки КОИ можно применять и избирательно: например, только для тех алгоритмических частей, которые являются наиболее чувствительными для криптоанализа. Для ГОСТ 28147-89 это работа с ключами, узлами замены, арифметическими операциями СМ1 и пересылками между ними. При таком ограниченном подходе применения РКД возможна экономия аппаратных ресурсов вычислителя. При этом снижение противокомпрометационного эффекта будет незначительным.

Замечательным техническим решением является все-таки реализация дублированного СКЗИ защищённым от компрометации вышеприведённым способом процессорного дублирования. На сегодня это возможно. Простейшее его исполнение возможно произвести в библиотеке логических элементов БИС или БМК (базовых матричных кристаллов) типа ПЛИС, в которой обе процессорные криптосхемы работают синхронно, но независимо друг от друга. То есть оба устройства выполняют функции шифрования. Одно устройство ведёт их в прямом коде, а другое — в обратном. При их абсолютной монокристальной синхронизации обеспечиваются условия РКД [17], а в качестве важного попутного эффекта возможно получение его постоянного функционально-динамического контроля операций шифрования.

3. В [20] представлены варианты противокомпрометационной защиты от атак по времени. Это существенно в алгоритмах,

использующих умножение, деление, возведение в степень и битовые операции над произвольным числом битов. То есть атака основана на предположении, что различные операции выполняются в устройстве за различное время в зависимости от входных данных. Измеряя время вычислений и проводя статистический анализ входных данных и КОИ, можно получить полную или частичную информацию о КОИ в целом или о её составных частях. Защита достигается за счёт временной нормализации выполнения указанных процедур. То есть все этапы шифрования в устройстве должны выполняться за одинаковое время. Добиться этого можно следующими способами:

- добавление фиксированной задержки: если известна аппаратная реализация, то можно рассчитать время выполнения каждой операции и уравнять их (операции), добавив фиксированные задержки [21];
- выполнение одновременно нескольких возможных операций [17, 22]: например, если в какой-то момент времени выполнения алгоритма должно производиться умножение и возведение в квадрат, то должны выполняться обе эти операции, которые по логике должны маскировать друг друга.

К сожалению, этот вид защиты СКЗИ достаточно сложен и трудоёмок в реализации, а для ГОСТ 28147-89 его можно просто исключить.

Альтернативой фиксированной задержке является как раз создание защитного недетерминированного вычислительного процесса (НДТ ВП) функций шифрования и их контроля [24].

Суть его заключается в следующем.

Перед запуском штатного алгоритма СКЗИ ГОСТ 28147-89 для выполнения функций криптопреобразований с целевыми данными запускается этот же алгоритм для обработки шумовых данных (случайных чисел) от качественного генератора случайных чисел (ГСЧ). При этом в качестве ключа также используются данные того же ГСЧ, но с другой позиции или из другого буферного блока. Число выполняемых раундов обработки шумовых данных алгоритмом ГОСТ 28147-89 определяется счётчиком этих

раундов, содержимое которого является случайной функцией ГСЧ в пределах отведённых границ. Верхняя граница счётчика должна быть предварительно вычислена исходя из требований к классу защищённости от компрометации СКЗИ. Счётчик случайных раундов обновляется каждый раз после окончания вычисления блока целевых данных — 64 бит. Соответственно, весь вычислительный процесс криптообработки целевых данных конкретного сообщения распределён на временной оси его шифрования неравномерно в соответствии с функцией ГСЧ.

На реализацию одного акта шифрования (дешифрования) выделяется временной ресурс T, который кратен времени реализации τ одного раунда и в среднем может быть равен 64 раундам:

$$T = N \cdot \tau, \text{ где } 32 < N \leq 64.$$

В качестве счётчика может использоваться 32-разрядный регистр сдвига, в который заносится 32-битовое (как вариант) случайное число. Это случайное число представляет собой шкалу тактирования «ложных» и «истинных» раундов. «Истинные» раунды реализуются в момент появления единичного бита шкалы тактирования, в остальных случаях реализуются «ложные» раунды. Временная недетерминированность определяется как число сочетаний C^{32}_{N}, где N в среднем равно значению 64.

Тогда временная недетерминированность (неопределённость) раунда определится как $t_{ндт} \leq 10^{-54}$.

Реальное число раундов для выполнения алгоритма ГОСТ 28147-89 может быть меньше или больше значения числа раундов 64 на величину Δ, определяющую значение допустимого преобладания соответствующего критерия. По окончании формирования 64-битного блока гаммы шифра делается новое заполнение тактового регистра.

Порядок формирования случайного числа (шкалы тактирования) может быть различным в зависимости от временных и аппаратных ресурсов.

Временная недетерминированность не даёт возможности криптоаналитику выполнять продуктивно криптоанализ из-за невозможности засинхронизировать начало и последующие раунды криптообработки каждого 64-битного блока формирования гаммы шифра. В принципе, НДТ ВП можно соотнести с некоторым стеганографическим эффектом, где в случайный недетерминированный процесс криптообработки случайных данных по случайному закону вложены блоки криптообработки штатно-целевых данных. Однако следует отметить, что для обеспечения НДТ ВП криптообработки СКЗИ должно обладать достаточным быстродействием, чтобы процесс шифрования не тормозил канальную скорость передачи данных, если это касается передачи зашифрованных данных. Сам НДТ ВП не оказывает влияния на процедуры шифрования информации. Соответственно, аппараты засекречивания информации, работающие друг на друга в сети, не обязаны иметь одинаковые временные планы НДТ ВП.

Более качественная схема НДТ ВП работает, если параллельно (в целях обеспечения контролепригодности) запускаются два СКЗИ, каждый из которых работает в своём режиме НДТ ВП. В этом случае информационная недетерминированность в составе ПЭМИН имеет более качественное зашумление КОИ. То есть имеет место и временное зашумление на временной оси, и физическое пространственное электромагнитное зашумление по принципу суперпозиции от двух вычислительных процессов.

Особо чувствительными к компрометации элементами являются любые ключи СКЗИ (инициализации, ГСЧ, ввода/вывода, доставки, хранения, доступа, долговременные рабочие, производные, сеансовые, масочные и другие ключи, которые могут использоваться для функций защиты). Общей для всех видов и типов ключей и исходной информации для них является необходимость устойчивой защиты против явной и неявной компрометации в соответствии с предписанными требованиями, которые предъявляются к технике шифрования. Данный вид защиты ключей должен обеспечиваться на всех жизненных этапах существования защищённой/засекреченной информации.

В данной статье обсуждаются ключи, ориентированные на применение в СКЗИ ГОСТ 28147-87, то есть симметричные ключи.

Основным условием защиты ключа, а в общем случае ключевой информации (КИ) или ключевых данных, является максимальное (по возможности) отделение её КИ от субъекта, будь то человек или процесс.

Ранее, по крайней мере до появления СКЗИ ГОСТ 28147-87 и разработки электронных ключевых носителей информации, применялась почти единственная, помимо электрофизических мер, организационная технология защиты КИ от компрометации — разделение секрета. То есть шифровальные системы строились таким образом, что его основное звено — ключ определялся двумя (в общем случае несколькими) частями. Например, ключ на основе перфоленты мог состоять из двух её частей, из которых формировался общий ключ посредством конкатенации или сложения по модулю 2 этих составных частей либо какой-то другой алгоритмической процедуры. При этом мощность ключа определялась таким образом, что, будучи скомпрометированными одной из ключевых частей, шифровальное устройство или система могли обеспечивать гарантированную криптозащиту в соответствии с заданным классом криптографической стойкости. Организационная составляющая определялась тем, что составные части перфоленты распечатывались из пакетов и вводились в шифрующее устройство двумя ответственными лицами. Считалось, что компрометация одновременно обеих составных частей ключа достаточно мала. Но, тем не менее, эта вероятность существовала, так как человек работал с частью ключа и имел возможность видеть эту часть, которую он вводил в шифрующее устройство через перфоленточное устройство ввода ключей.

Современные технологии управления и работы с ключами позволяют освободиться от самого ненадёжного компрометирующего элемента — человека. При этом принцип разделения секрета продолжает или может оставаться.

Современные технологии защиты ключей при работе с ними (в сочетании с существующими технологиями) могут быть следующими.

- Формирование кодов ключей, их разделение (как секрета) и запоминание в носителях КИ и/или в самих шифрующих устройствах производится электронным способом без возможности их физического наблюдения и регистрации человеком. (Во внимание не принимаются особые случаи, когда ввод специального ключа в СКЗИ или шифрующее устройство производится вручную с пульта управления. В этом случае продолжают работать правила разделения секрета. Последнее не касается ввода пароля.)
- Применяются алгоритмические и информационные методы противокомпрометационной защиты при вводе КИ, её хранении, обработки и формировании видов/типов исполнительных ключей и использования их в процедурах шифрования.
- Электрофизические методы защиты продолжают работать и определяются конкретными требованиями, предъявляемыми к средствам защиты при их разработке.
- Организационные меры особенно тщательно выполняются при выработке исходной КИ в соответствии с требованиями, определяемыми приказом № 152 ФСБ [26] и рекомендациями 8-го центра ФСБ России № 149/54-144: [8].

Рассмотрим алгоритмические и информационные методы противокомпрометационной защиты КИ.

При выработке, например, на станции ключевого обеспечения и передаче по интерфейсным цепям КИ или канальным линиям связи целесообразно применять методы алгоритмического и кодового зашумления в соответствии с алгоритмами, описанными выше. В настоящее время широко применяются методы передачи ключей — это передача их в зашифрованном и/или замаскированном виде. При этом ключ шифрования/маскирования ключей может являться как раз элементом разделения секрета, который должен вводиться в СКЗИ или в шифрующее устройство другим лицом. Доставляться ключ шифрования ей

к СКЗИ может каналом, отличным от канала доставки первого зашифрованного ключа и желательно не синхронизованного с доставкой первого. Ключ шифрования ключей, как правило, называется ключом доставки ключей. Данный ключ может носить характер долговременного ключа, так как накопление статистики по нему — достаточно сложная задача в силу непредсказуемости начальной ключевой загрузки СКЗИ и редкости её смены. Единственный предсказуемый момент может быть, когда отрабатывается контрольная процедура аппарата шифрования или СКЗИ перед передачей его в эксплуатацию. В этом случае ключи могут применяться как технологические и на штатно-рабочие функции они никак не должны влиять.

Следующим актом криптонадёжного скрытия КИ в памяти процессора, выполняющего функции криптообработки, является запись в память и хранение ключа, зашифрованного на ключе хранения [22, 23]. При этом ключ хранения может быть также вводимым извне либо иметь качественное формирование хотя бы по тому же алгоритму ГОСТ 28147-89. При этом формирование ключа хранения может производиться из собственных ресурсов СКЗИ (от собственного ГСЧ) и не выводиться из последнего наружу. Тем самым будет обеспечена абсолютная недоступность к его прочтению. Если СКЗИ выполнено для решения задач многопользовательского режима, то для каждого пользователя может быть создан свой ключ хранения, а вся совокупность этих ключей будет организована в ключевой файл, который, в свою очередь, будет зашифрован на одноразовом внутреннем ключе СКЗИ. Он также должен храниться в СКЗИ и каждый раз перешифровываться при раскрытии ключевого файла. Подобная схема реализована, работает и описана в [26]. Следует отметить, что сам ключ файла хранится в памяти СКЗИ под динамической маской [23, 26], стирание которой (в случае необходимости) позволяет исключить возможность какого-либо доступа к защищённой информации в СКЗИ, так как последняя останется закрытой криптографическим шифром, от которого ключ будет стёрт.

Криптосхема ГОСТ 28147-89 позволяет иметь несколько технических решений маскирования ключевой информации. Как-то:

а) маскирование ключа после приёма через порт ввода и размещения его в ключевой памяти. При этом выполняются предваряющие процедуры по проверке его достоверности, очистки от ключа доставки, зашифрования на ключе хранения, формирования динамической маски, последующего маскирования и выполнения процедуры собственно хранения. При выполнении штатно-целевых процедур по ГОСТ 28147-89 ключ извлекается из памяти, очищается от всех «масочных наслоений» и пересылается в рабочую область памяти или сумматора для выполнения рабочих криптографических функций. Сам процесс криптографических вычислений производится с открытым (незашифрованным) ключом. Это обстоятельство (работа чистого ключа и его пересылки) является уязвимостью шифра, так как возможно существование следов КИ в ПЭМИН. Устранение данной уязвимости возможно, если применить другой вариант маскирования, описываемый ниже;

б) применение замаскированного ключа в процессе выполнения криптографических функций. Ключ хранится в рабочем блоке памяти в замаскированном виде. Процедуры промежуточных вычислений гамм шифра или самого шифра производятся под замаскированным ключом. Снятие маски производится перед обращением в память узла замены. К этому моменту ключ уже обработан/замешан с данными предварительных криптографических преобразований. Маска, маскирующая ключ, может вырабатываться в СКЗИ от собственного ГСЧ и не является доступной для внешней среды (по отношению к СКЗИ). Данный метод маскирования ключа при криптообработке с учётом его замаскированного ввода практически полностью исключает возможность получить неявный компрометационный (через ПЭМИН) фактор рабочего ключа. В этом плане существенно (в разы) может быть повышена его живучесть.

Продление жизни рабочих долговременных ключей, вводимых в СКЗИ или шифрующее устройство, с точки зрения защиты их от неявной компрометации может осуществляться

благодаря обоснованной разработке ключевой структуры. Последнее, в свою очередь, должно опираться на схему шифрованной связи (как сетевого продукта) либо на организацию защищённого (шифрованного) документооборота (имеется в виду электронного) и соответствующие модели нарушителей.

Криптографически защищённые системы, как правило, работают в пространстве человеческого фактора, который, в свою очередь, является самым ненадёжным её элементом. А посему корректно организованная ключевая структура должна обеспечивать необходимую продолжительность функционирования долговременным ключам от неявной компрометации и ключевой системе в целом при отдельных явных компрометациях ключей абонентов или пользователей. Данным требованиям удовлетворяет построение многоуровневой ключевой структуры, основу которой составляют долговременный рабочий ключ или система ключей. Данный рабочий ключ или их система не являются штатно-исполнительной на конкретный момент времени шифрования информации. Они являются первообразными, то есть исходной ключевой информацией для формирования производных ключей. Последние формируются как функция от исходной КИ и ряда параметров организации связи или управления данными. В качестве параметров (в зависимости от системы связи) могут служить вид/тип связи (широковещательная, групповая или направленческая), виды и форматы адресации и их модификаторы, признаки приёма/передачи, параметры времени, случайные посылки и др. Отдельные параметры или их совокупности в алгоритме ГОСТ 28147-89 могут использоваться как синхропосылка «режима простой замены».

В соответствии с параметрами в СКЗИ или шифраторе вырабатываются производные ключи различных уровней, которые могут быть ориентированы на различные объёмы шифрования информации. После обработки допустимого объёма шифрования информации на производном ключе последний должен быть переформирован. В системе, использующей алгоритм ГОСТ 28147-89, как правило, предполагается, что все ключевые преобразования производятся на том же ГОСТ 28147-89. Данная реализация хорошо представлена в [26]. Применение производных

ключей позволяет реже обращаться к базовой рабочей КИ. Тем самым исключается возможность её наблюдать и накапливать через ПЭМИН. А то, что период обращения к рабочим ключам носит случайный, несинхронизируемый характер, обеспечивает низкую вероятность их перехвата и соответствующее низкое накопление статистики по ним для криптоанализа. Это также является положительным качеством системы защиты.

В этом плане производные ключи являются организационно-защитными для исходной КИ. Каждый уровень производного ключа, в свою очередь, является защитой для ключа вышестоящего уровня, так как уменьшает частоту обращения к нему. Ключом нижнего уровня, а в некоторых случаях самого нижнего уровня является сеансовый ключ. То есть ключ, на котором ведётся защищённая связь или передача данных. Он формируется на один сеанс связи. Если работает система низовой радиосвязи, то это один акт передачи речевого сообщения либо блока данных в одну сторону. Пример — одно нажатие тангенты абонентской радиостанции на одной из сторон.

Обеспечение контролепригодности криптографической защиты

Контролепригодность [11] криптографической защиты, реализуемая в СКЗИ, строится в основном на использовании:

- системы контроля СКЗИ;
- системы контроля электропитания СКЗИ;
- системы защиты СКЗИ на основе стирания КИ и КОИ, хранящейся во внутренних элементах СКЗИ, срабатывающей по дистанционной команде или по команде оператора с пульта управления СКЗИ (функция вводится, как правило, для защиты СКЗИ от возможной явной компрометации).

Система контроля СКЗИ

Система контроля включает в себя:

- пусковой контроль, который осуществляется при включении СКЗИ;

- оперативный контроль, который проводится в ходе обработки и/или приёма и передачи информации, например, по радиоканалу;
- периодический (регламентный) контроль на ключах, вводимых извне.

Пусковой контроль по включению питания осуществляет тестирование элементов СКЗИ и платформы, в которую оно встроено. Контроль, как правило, строится на прокрутке штатно-целевых программ, с обработкой контрольно-тестовых данных. Он включает в себя проверку работоспособности функциональных узлов и режимов работы СКЗИ, отсутствие искажений программного обеспечения вычислителя, если таковой входит в состав СКЗИ или, наоборот, СКЗИ входит в состав вычислительной платформы, для которой оно выполняет защитные функции. Контролируются функции обеспечения достоверности вычислительных режимов (контрольные вычисления, дублирующие функции, если таковые встроены), формирования гамм шифра, КИ, ГСЧ, включая средства оценки его качества, а также блокирующих элементов, предотвращающих выдачу КОИ в любой канал, который потенциально может быть доступным нарушителю.

Самоблокируемый оператор сравнения

Если СКЗИ выполнено программным способом, важным элементом контрольного тестирования является проверка самоблокируемого оператора сравнения *if* [27]. В силу его значимости имеет смысл рассмотреть этот элемент более детально.

Модель оператора сравнения *if* (язык С) имеет вид.

If (ВЫРАЖЕНИЕ) ОПЕРАТОР.

Оператор *If* работает в соответствии со следующей моделью:

1) вычисляется ВЫРАЖЕНИЕ;

2) если ВЫРАЖЕНИЕ является ненулевой величиной, то выполнятся ОПЕРАТОР,

3) если ВЫРАЖЕНИЕ равно нулю, то ОПЕРАТОР не выполняется.

Для приведённой модели отказов оператора *If* будем рассматривать следующие варианты его поведения:

1) оператор *if* вырождается в ОПЕРАТОР;
2) оператор *if* вырождается в пустой оператор;
3) оператор *if* инвертируется, то есть, если ВЫРАЖЕНИЕ обращается в ноль, выполнятся ОПЕРАТОР, в противном случае ОПЕРАТОР не выполняется.

Для данной модели отказов производится построение программы сравнения массивов данных средствами языка С, которая возвращает величину *TRUE*, если массивы поэлементно равны, а оператор *if* не вырождается в один из переведённых вариантов, и величину *FALSE*, если массивы различны, либо оператор *if* вырождается в соответствии с принятой моделью. Программа для приведённой выше модели отказов, осуществляющая проверку факта, что переменная A = 0, имеет следующий вид:

```
if (0) return FALSE; // проверка по п.п. 1,2
if (7)  {
        if (A) return FALSE;
        return TRUE;
        }
return FALSE;// проверка по п.2
```

На основе вышеприведённого фрагмента программы строится программа по схеме трёх успешных сравнений. Пусть *A, B* и *C* — разные операторы сравнения, возвращающие 0 при равенстве сравниваемых величин. Нижеприведённая программа демонстрирует построение надёжной программы сравнения по этой схеме.

```
if (0) return FALSE;
if (7)  {
        if (A) {
                if (!B)
                        if (!C) return TRUE;
                return FALSE;
                }
        }
return FALSE;
```

Для приведённой программы делается вывод, что если вероятность опасного отказа оператора сравнения равна P (1), то вероятность события, заключающегося в том, что процедура сравнения возвращает величину *TRUE* при условии неравенства сравниваемых массивов и при соответствии модели отказов оператора *if* пп. 1, 2 и 3 будут составлять (по крайней мере) величину $P(1)^2$ [27].

Контроль отсутствия искажения (навязанной или случайной трансформации) ПО проводится как для СКЗИ, так и для платформы, в которую оно встраивается. Контроль общего ПО платформы может выполняться по контрольной сумме. Контроль ПО СКЗИ в соответствии с требованиями, которые предъявляются к ним, выполняется по контрольной имитозащитной сумме на контрольном ключе. CRC и имитозащитная сумма входят в состав установочных данных при загрузке ПО. Проверяются процедуры стирания КОИ, масочные функции и их динамика. Контролируется формирование специальных служебно-командных процедур, если таковые определены для СКЗИ.

Интерфейсные линии и каналы СКЗИ и изделия, в которое оно встраивается, могут проверяться прямым или условным замыканием каналов «сам на себя».

Следует отметить, что контроль по включению питания проводится и при выполнении операции Reset вне зависимости от того, пультовая это операция или командно-дистанционная.

Оперативный контроль

Оперативный контроль, как было сказано выше, предназначен для обеспечения криптографической надёжности в процессе выполнения криптографических функций СКЗИ. Он проводится в непосредственном процесссе криптографической обработки и/или приёма и передачи информации. Его задача — обеспечить достоверный приём, обработку и выдачу информации в открытый канал. Оперативный контроль приёма закрытых целевых данных осуществляется посредством вычисления криптографической имитопосылки. Заголовочная посылка (синхропосылка) во многих случаях не шифруется.

Её достоверность приёма обеспечивается помехоустойчивым кодированием либо её мажорированием. Наиболее важной и ответственной частью приёма/передачи является направление выдачи информации в зашифрованном виде. В случае возникновения каких-либо аппаратных и/или программных инцидентов, вызванных сбоями, отказами в аппаратно-программной среде, шифратор должен обеспечивать гарантированную блокировку выдачи информации в открытый канал. Современная реализация оперативного контроля строится на процедурном дублировании криптографических процессов и просчёте контрольно-тестовых криптографических примеров. При этом дублирование может быть выполнено как аппаратным (аппаратно-программным) способом, так и программно-временным методом.

Программно-временной контроль процесса шифрования информации

В шифраторе используется алгоритм ГОСТ 28147-89. Криптоалгоритм реализуется программно на цифровом процессоре. Основным элементом инженерно-криптографической защиты перед выполнением функции выдачи зашифрованных данных является программно-временное дублирование процесса шифрования и сравнение его результатов перед выдачей зашифрованной информации в канал связи.

Схематично временная диаграмма процесса дублированного шифрования информации представлена на рис. 2.

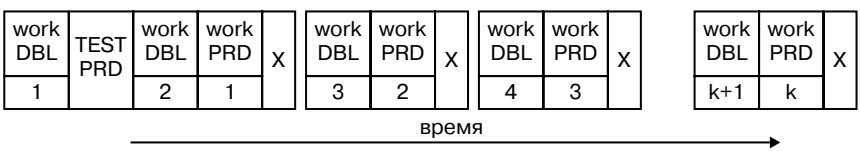


Рис. 2. Временная диаграмма процесса дублированного шифрования/расшифрования информации

Здесь work PRD и work DBL — временные поля циклов работы основного и дублирующего шифраторов соответственно; TEST PRD — временное поле прогона шифратора на тестовом

примере (зашифрование/расшифрование в режиме временного дублирования фиксированного открытого текста на известном тестовом ключе и сравнение полученного результата с заранее известным эталонным кодом). По положительному результату сравнения должна быть сформирована разрешающая команда на вывод информации в открытый канал, например, по логической схеме, представленной ниже на рис. 3 (временное поле X на рис. 2). В поле X помещается значение/результат от сравнения блоков гаммы шифра, выработанных основным и дублирующим шифратором. Если результат сравнения является отрицательным, то информация в канал не выдаётся, а сам канал блокируется для её выдачи.

Рассмотрим формирование команды на вывод информации в канал.

Программное обеспечение ЦП не содержит явной команды на вывод информации в канал. Команда на вывод каждого зашифрованного блока данных (канального пакета) формируется по положительным результатам тестов контрольного просчёта контрольных данных (контрольной переменной) и результатам сравнения байтов криптограммы, выработанных на основном и дублирующем циклах работы шифратора.

Эта команда формируется в ходе оперативного контроля процесса шифрования с использованием динамически изменяемой контрольной переменной. Формирование контрольной переменной осуществляется при:

- успешном завершении каждой из функций пускового контроля (по включению питания СКЗИ) либо начале сеанса связи;
- успешном завершении каждой из функций оперативного контроля;
- успешном прохождении теста передающего шифратора.

Длина контрольной переменной (как пример) составляет 16 бит и динамически, с некоторого начального значения, «прошиваемого» в энергонезависимую память, изменяется путём циклического сдвига на 1 бит при выполнении каждого из вышеперечисленных условий. Команда на вывод информации в канал связи формируется по результатам сравнения знаков

(байтов) криптограммы, выработанной в основном и дублирующем циклах работы шифраторов по логической схеме, приведенной на рис. 3.

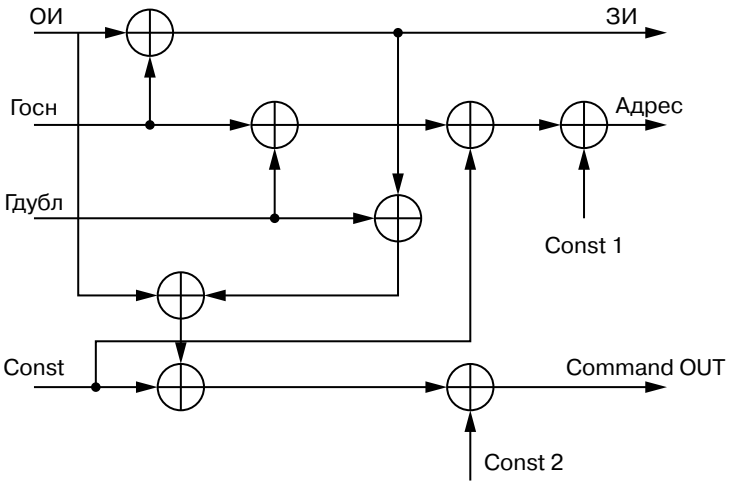


Рис. 3. Формирование команды (как вариант) на выдачу в канал связи зашифрованной достоверной информации (ОИ и ЗИ — открытая и закрытая информация соответственно; Адрес — адрес сопровождения выходной информации; Command OUT — команда сопровождения выдачи достоверной ЗИ либо блокировки канала выдачи в случае её недостоверного результата (не сравнения данных ЗИ шифраторов); Госн — блок гаммы, выработанный основным шифратором; Гдубл — блок гаммы, выработанный дублирующим шифратором; Const — общая константа формирования адреса ЗИ и Command OUT; Const 1 — константа 1, дополняющая формат адреса достоверной закрытой информации; Const 2 — константа 2, дополняющая формат команды Command OUT, которая выдается при получении недостоверной ЗИ)

Периодический (регламентный) контроль ПО на основе вводимых данных и ключей

Данный контроль, как правило, проводится уполномоченным оператором визуально либо с применением специального внешнего оборудования.

Контроль состоит из следующих процедур:

1) загрузки в СКЗИ тестовых криптографических данных (тестового криптографического ключа, тестовых данных, подлежащих криптографической обработке — зашифрованию/расшифрованию);
2) выполнения просчёта имитовставки от программного кода, хранимого в памяти устройства ЦП, и передачи на внешнее устройство или устройство визуального отображения результатов просчёта для контроля оператором;
3) выполнения в СКЗИ процедур дублированного зашифрования/расшифрования тестовых данных (вводимых извне) в рабочих алгоритмах ГОСТ 28147-89 и передачи на внешнее устройство или устройство визуального отображения результатов для контроля оператором;
4) индикации полученных от СКЗИ результатов контроля и сравнения оператором этих результатов с заранее известными эталонными значениями.

Индицируемые результаты позволяют оператору принять решение о работоспособности СКЗИ и целостности его программного кода.

Заключение

Данная статья фактически является рекомендательным материалом или рабочим руководством для разработчиков криптошифраторов высокой противокомпрометационной стойкости и контролепригодности. То есть описываемая методика с учетом конкретных специальных требований, предъявляемых к технике защиты информации, позволяет разрабатывать и производить информационные криптошифраторы с обеспечением высокого уровня собственной безопасности. Причем высокие качества шифраторов в основном достигаются за счёт применения специального равновесного кодирования, которое в целом не увеличивает объемы оборудования для построения высоконадёжных (дублированных [26, 28]) шифраторов.

Литература

1. Государственный стандарт Союза ССР. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. ГОСТ 28147-89 ИПК. — Издательство стандартов, Москва.
2. Anderson R., Bond M., Clulow J., Skorobogatov, S. Cryptographic processors — a survey (англ.) // Proceedings of the IEEE : журнал. — 2006. — В. 2. — Т. 94. — С. 357–369.
3. Дж. Барнс Электронное конструирование: методы борьбы с помехами: Пер. с англ. — Мир, 1990. — 238 с.
4. FIPS PUB 140-2 change notices (12-03-2002) Federal information processing standards publication (Supercedes FIPS PUB 140-1, 1994 January 11) security requirements for cryptographic modules.
5. YongBin Zhou, DengGuo Feng. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing (англ.) // Information Security Seminar WS 0607. — 2006.
6. Jean-Jacques Quisquater, Francois Koeune. Side Channel Attacks // Start of the art, October 2010.
7. Жуков А. Е. Криптоанализ по побочным каналам (Side Channel Attacks) Доклад на конференции РусКрипто 2006 (2006).
8. Методические рекомендации 8-го центра ФСБ России от 21.02.2008 г. № 149/54-144.
9. Security Supplement to the Software Communications Architecture Specification // JTRS-5000 SEC, V. 3.0 August 27, 2004.
10. Security Supplement to the Software Communications Architecture Specification Attachment 1 Security Application Program Interface Service Definition // JTRS-5000SEC Security API Service Definition, rev. 3.0.
11. Костогрызов А. И., Липаев В. В. Сертификация качества функционирования автоматизированных информационных систем. — М., 1996. — 280 с.
12. Липаев В. В. Надежность программных средств. Серия «Информатизация России на пороге XXI века». — М.: СИНТЕГ, 1998. — 222 с.

13. Липаев В. В. Системное проектирование сложных программных средств для информационных систем. Серия «Информатизация России на пороге XXI века». — М.: СИНТЕГ, 1999. — 224 с.
14. Щербаков А. Ю. Разрушающие программные воздействия. — М.: Издательство «ЭДЕЛЬ», 1992.
15. Прокофьев И. В., Шрамков И. Г., Щербаков А. Ю. Введение в теоретические основы компьютерной безопасности. — М.: Издательство МГИЭМ, 1998.
16. Зверев Е. М., Андрущенко А. С., Комиссаров А. В., Щербаков А. Ю. Построение самоблокирующей программной среды в средствах криптографической защиты // Известия ТРТУ. Тематический выпуск. Материалы V Международной научно-практической конференции «Информационная безопасность». — Таганрог: Издательство ТРТУ, 2005. — № 4 (48). — С. 173–181.
17. Зверев Е. М. Применение равновесных кодов для обработки информации // ЦОНТИ «ЭКОС». Научно-технический сборник. Специальная техника средств связи. Сер. «Общетехническая». — 1987. — Вып. 2 (31). — С. 22–28.
18. Курант Р., Роббинс Г. Что такое математика? /Перев. с английского А. Н. Колмогорова. — 3-е изд., испр. и доп. — М.: МЦНМО, 2001. — 568 с.
19. Вавилов Е. Н., Портной Г. П. Синтез схем электронных цифровых машин — М.: Советское радио, 1963.
20. Процесор AMD Athlon 64 XP 2800+ Advanced Micro Devices, Inc. http: //www/ amd/ru.
21. Лукашов И. Аппаратные шифраторы на отечественной элементной базе // Электроника: Наука, Технология, Бизнес, 6/2001.
22. J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestre, J.-J. Quisquater, J.-L. Willems. A practical implementation of the timing attack (англ.) // Proceedings of the The International Conference on Smart Card Research and Applications : сборник. — London, UK: Springer-Verlag, 1998. — С. 167–182.

23. YongBin Zhou, DengGuo Feng. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing (англ.) // Information Security Seminar WS 0607. — 2006.
24. Баталов Б. В., Зверев Е. М., Малютин А. В. Методы создания временной недетерминированности вычислительного процесса обработки в микропроцессорных устройствах // ЦОНТИ «ЭКОС». Научно-технический сборник. Специальная техника средств связи, серия общетехническая. — 1987. — Вып. 2 (31). — С. 2–14.
25. Приложение к приказу ФАПСИ от 13 июня 2001 г. № 152 «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
26. Зверев Е. М. Криптографическая защита каналов связи ССС «Сокол—Банкир» с использованием платы «Криптон-3» // Бюллетень Центрального банка России, 1995.
27. Домашев А. В., Грунтович М. М., Попов В. О., Правиков Д. И., Прокофьев И. В., Щербаков А. Ю. Программирование алгоритмов защиты информации: Учебное пособие. Издание 2-е исправленное и дополненное: — М.: Издатель Молгачева С. В., издательство «Нолидж», 2002. — 552 с.
28. Фирма «АНКАД» — 25 лет на службе обеспечения информационной безопасности России / Под ред. Ю. В. Романца — 2016.
29. Jean-Jacques Quisquater and David Samyde. ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards (англ.) // E-SMART ‘01 Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security: сборник. — Springer-Verlag, 2001. — Т. 2140. — С. 200–210.
30. Karine Gandolfi, D. Naccache, C. Paar, Karine G., Christophe Mourtel, Francis Olivier. Electromagnetic Analysis: Concrete Results (англ.) // Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems : сборник. — Springer-Verlag, 2001. — С. 251–261.

31. Barenghi A., Bertoni G., Parrinello E., Pelosi G. Low Voltage Fault Attacks on the RSA Cryptosystem (англ.) // Workshop on Fault Diagnosis and Tolerance in Cryptography: сборник — 2009. — С. 23–31.
32. Vincent Carlier, Hervé Chabanne, Emmanuelle Dottax, Hervé Pelletier, Sagem Sa. Electromagnetic Side Channels of an FPGA Implementation of AES (англ.) // Computer as a Tool, 2005. EUROCON 2005: сборник. — 2005.
33. E. De Mulder, P. Buysschaert, S. B. Örs, P. Delmotte, B. Preneel, I. Verbauwhede. Electromagnetic Analysis Attack on a FPGA Implementation of an Elliptic Curve Cryptosystem (англ.) // EUROCON: Proceedings of the International Conference on «Computer as a tool : сборник. — 2005. — С. 1879–1882.
34. Pierre-alain Fouque, Gaëtan Leurent, Denis Réal, Frédéric Valette. Practical Electromagnetic Template Attack on HMAC (англ.) // Cryptographic Hardware and Embedded Systems — CHES 2009: сборник. — 2009. — С. 66–80.

Публикуется впервые


ОТЕЧЕСТВЕННАЯ
ЭЛЕКТРОННАЯ
ВЫЧИСЛИТЕЛЬНАЯ
ТЕХНИКА
ЛАУРЕАТА
Известия высших учебных заведений.
ЭЛЕКТРОНИКА
Zelenograd.ru
АКАДЕМИК
ИЗОБРЕТАТ
РАЦИОН

ГЛАВА 4

ПУБЛИКАЦИИ О В. М. АМЕРБАЕВЕ

В различных изданиях и в Интернете имеется множество публикаций о В. М. Амербаеве, что дополнительно свидетельствует о его высоком авторитете в научном обществе и огромном вкладе в развитие отечественной науки и её прикладного применения в народном хозяйстве, в оборонной технике. Поскольку статьи, как правило, в значительной степени (а часто и полностью) повторяют друг друга, из этого множества редакционная группа выбрала следующие.

— • —

Отечественная электронная вычислительная техника. Биографическая энциклопедия.

М.: Столичная энциклопедия, 2014. — С. 11.

Амербаев Вильжан Мавлютинович

Родился 25 апреля 1931 г. в г. Талды-Кургане Казахской ССР.

В 1954 г. окончил Казахский государственный университет по специальности «математика».

В 1955–1959 гг. — аспирант Математического института им. В. А. Стеклова АН СССР, где защитил диссертацию кандидата физико-математических наук.

В 1959–1963 г. — младший научный сотрудник, заведующий лабораторией вычислительной и машинной

Амербаев Вильжан Мавлютинович

математики при президиуме АН КазССР.

В 1967–1972 — начальник отдела специализированного вычислительного центра МЭП СССР, г. Зеленоград, ведущий разработчик модулярной арифметики (МА) для супер-ЭВМ 5Э53, работающей в системе остаточных классов.

В 1972–1978 — заместитель директора Института математики и механики АН Казахской ССР.

1978–1981 — заведующий кафедрой ЭВМ Московского института инженеров гражданской авиации.

1981–1987 — профессор кафедры высшей математики Московского института электронной техники.

В 1988–1993 — академик-секретарь отделения физико-математических наук АН КазССР (с 1991 г. Республики Казахстан — РК), член президиума АН РК.

В 1994–2007 г. ведущий научный сотрудник НПЦ «СПУРТ».

С 2007 г. и по настоящее время — профессор кафедры вычислительной техники МИЭТ и главный научный сотрудник Института проблем проектирования в микроэлектронике РАН, занимается теоретическими и прикладными исследованиями в области интрамодулярных вычислений: модулярной логарифметики, бимодульной МА, рекурсивной МА.

Математик, доктор технических наук (1971), профессор вычислительной математики (1973), академик НАН РК (1987).

Специалист в области компьютерной алгебры и цифровой обработки сигналов. Его математическая активность в области информатики связана с привлечением фундаментальных алгебраических структур для организации вычислений в целях достижения методами распараллеливания высоких показателей по быстродействию, надёжности и точности на вычислительных

средах специального назначения, повышения качества приборов (измерений) и сжатия визуальной информации.

В. М. Амербаев опубликовал более 120 научных трудов, в т. ч. 6 монографий. Им подготовлено 27 кандидатов и 3 доктора наук.

Награды

Медали: «За доблестный труд в ознаменование 100-летия В. И. Ленина» (1970) и «За трудовую доблесть» (1972).

Лауреат Государственной премии СССР по науке и технике (1991).

— • —

Большая биографическая энциклопедия

https://dic.academic.ru/
2009
https://dic.academic.ru/dic.nsf/enc_biography/3045/Амербаев

Амербаев, Вильжан Мавлютинович

Амербаев, Вильжан Мавлютинович (род. 25.4.1931) — советский математик, чл.-кор. АН КазССР (1972). Чл. КПСС с 1968. Род. в Талды-Кургане (КазССР). Окончил Казах. ун-т (1954), д-р физико-матем. наук (1971). Труды по операционному исчислению и теории арифметического кодирования информации.

— • —

Интернет-портал «Жизнь замечательных людей Казахстана»

http://www.zzl.kz/
http://www.zzl.kz/rubric/det/139/471/

Амербаев Вильжан Мавлютинович
(1931)

Математик, доктор физико-математических наук (1971), профессор (1973), академик НАН РК (1989), лауреат Государственной премии СССР по науке и технике (1991).

Окончил физико-математический факультет Казахского государственного университета в 1954 году по специальности «математика».

Окончил аспирантуру Математического института им. Стеклова АН СССР и защитил кандидатскую диссертацию на соискание учёной степени кандидата физико-математических наук на учёном совете МИАН СССР в 1963 году. Тема диссертации — «Численные методы обращения интегрального преобразования Лапласа».

Специалист в области компьютерной алгебры и цифровой обработки сигналов. Его математическая активность в области информатики связана с привлечением фундаментальных алгебраических структур для организации вычислений в целях достижения высоких показателей по быстродействию, надёжности, точности на вычислительных средах специального назначения, повышения качества приборов (измерений) и сжатия визуальной информации. Основные результаты — теория модулярного кодирования в кольце главных идеалов, цифровые методы отображения интегралов Лапласа, обобщённое операционное исчисление, новые и численные методы деконволюции. Выполнил большой цикл работ в области компьютерной алгебры и цифровых методов обработки сигналов. Результаты исследований отражены в 90 печатных работах и заявках на изобретения, в том числе в 6 монографиях.

В 1971 г. защитил докторскую диссертацию на учёном совете НПО «Элас» НЦ МЭП СССР (г. Москва) на тему «Вычисления в кольце главных идеалов и их приложения в вычислительной технике». В диссертации была разработана алгебраическая концепция параллельных вычислений, повышения надёжности вычислений посредством алгебраических методов введения избыточности, разработаны принципы арифметического

самокорректирующегося кодирования. Частные реализации этой концепции легли в основу проектирования арифметического процессора высокопроизводительной вычислительной системы. В 1977 г. получил звание профессора по кафедре вычислительной математики.

Лауреат Государственной премии СССР 1991 г.

Основные научные публикации относятся к областям теории кодирования, параллельных вычислений, помехоустойчивого арифметического кодирования, численных методов обращения интегральных преобразований Лапласа, сверхточных уравнений.

Монографии:

Основы машинной арифметики комплексных чисел. — Алма-Ата: Наука, 1970. — 248 с.

Обобщенные ряды Лаггера и операционное исчисление. — Алма-Ата: Наука, 1974. — 181 с.

Теоретические основы машинной арифметики. — Алма-Ата: Наука, 1976. — 323 с.

Распределение регулярных потоков сообщений в информационных системах. — Алма-Ата: Наука, 1980. — 143 с.

Параллельные вычисления в комплексной плоскости. — Алма-Ата: Наука, 1984. — 177 с.

Анализ и синтез лагеррованного спектра. — Алма-Ата: Наука, 1984. — 180 с.

— • —

Сайт Национального исследовательского университета «МИЭТ»

https://miet.ru/
https://miet.ru/person/10547

Амербаев Вильжан Мавлютинович (1931–2014)
академик Национальной академии наук Казахстана,
доктор технических наук, профессор

Краткая биография

Окончил Казахский государственный университет, физико-математический факультет по специальности «математика» в 1954 году.

Окончил аспирантуру Математического института им. Стеклова АН СССР и защитил кандидатскую диссертацию на соискание учёной степени кандидата физико-математических наук на учёном совете МИАН СССР в 1963 году. Тема диссертации — «Численные методы обращения интегрального преобразования Лапласа».

В 1971 г. защитил докторскую диссертацию на учёном совете НПО «Элас» НЦ МЭП СССР (г. Москва), на тему «Вычисления в кольце главных идеалов и их приложения в вычислительной технике». В диссертации была разработана алгебраическая концепция параллельных вычислений, повышения надёжности вычислений посредством алгебраических методов введения избыточности, разработаны принципы арифметического самокорректирующегося кодирования. Частные реализации этой концепции легли в основу проектирования арифметического процессора высокопроизводительной вычислительной системы.

В 1977 г. получил звание профессора по кафедре вычислительной математики.

Лауреат Государственной премии СССР.

Научная деятельность, научные интересы

- цифровая обработка данных;
- цифровая реализация интегральных образований и их обращений, включая сверхточные интегральные преобразование;
- методы цифровой аподизации в задачах дистанционного зондирования, повышения разрешающей способности приборов, инвариантных к сдвигу;

- алгебраические методы повышения производительности вычислений в кольце целых чисел, гауссовых чисел и кватернионов;
- прикладные задачи алгебраического кодирования, включая помехоустойчивость;
- теоретические задачи криптологии, организация вычислений в квазигруппах, цифровые методы детерминированного хаоса в задачах криптографии и задачах математического моделирования генетических последовательностей.

Научно-производственная деятельность

- заведующий лабораторией в 1963–1971 гг.;
- заместитель директора института математики АН КазССР в 1972–1977 гг.;
- заведующий кафедрой ЭВМ МИИГА с 1977 по 1981 гг.;
- академик-секретарь отделения физико-математических наук АН КазССР, член президиума АН КазССР в 1987–1993 гг.

Принадлежность к научным школам по разрабатываемой проблематике научно-исследовательской деятельности

- школа академика А. А. Дородницына и профессора В. А. Диткина;
- школа академика АН КазССР К. В. Персидского;
- школа чл.-корр. АН СССР Л. Н. Преснухина.

Учебная деятельность

Под руководством В. М. Амербаева 23 человека защитили кандидатские диссертации; консультировал работу над 3 докторскими диссертациями

Публикации

Основные научные публикации относятся к областям теории кодирования, параллельных вычислений, помехоустойчивого арифметического кодирования, численных методов обращения интегральных преобразований Лапласа, сверхточных уравнений.

Монографии

- Основы машинной арифметики комплексных чисел. — Алма-Ата: Наука, 1970. — 248 с.
- Обобщенные ряды Лагерра и операционное исчисление. — Алма-Ата: Наука, 1974. — 181 с.
- Теоретические основы машинной арифметики. — Алма-Ата: Наука, 1976. — 323 с.
- Распределение регулярных потоков сообщений в информационных системах. — Алма-Ата: Наука, 1980. — 143 с.
- Параллельные вычисления в комплексной плоскости. — Алма-Ата: Наука, 1984. — 177 с.

Анализ и синтез лагеррованного спектра[1]. — Алма-Ата: Наука, 1984. — 180 с.

— • —

«Википедия», свободная энциклопедия

https://ru.wikipedia.org/
https://ru.wikipedia.org/wiki/
Амербаев,_Вильжан_Мавлютинович

ВИКИПЕДИЯ
Свободная энциклопедия

[1] Монография «Анализ и синтез лагеррованного спектра», упомянутая в этой и других статьях о В. М. Амербаеве (в статьях иного рода не обнаружена), неизвестна его коллегам и ни в библиотеках, ни в Интернете не обнаружена, в библиографию не включена. Коллеги вспоминают, что эта монография была выпущена под наименованием «Численный анализ лагерровского спектра».

Амербаев Вильжан Мавлютинович

Дата рождения	25 апреля 1931
Место рождения	Талды-Курган, Алматинская область, Казахская АССР, РСФСР, СССР
Дата смерти	14 декабря 2014 (2014-12-14) (83 года)
Место смерти	Зеленоград, Москва, Россия
Страна	СССР Казахстан
Научная сфера	математик
Место работы	Институт математики и механики АН Казахской ССР Московский институт электронной техники Институт теоретической и прикладной математики НАН РК
Альма-матер	Казахский государственный университет имени С. М. Кирова
Учёная степень	доктор физико-математических наук (1971)

Учёное звание	профессор (1973), член-корреспондент АН Казахской ССР (1972), академик НАН РК (1989)
Научный руководитель	Дородницын Анатолий Алексеевич, Персидский Константин Петрович, Преснухин Леонид Николаевич
Известен как	Специалист в области компьютерной алгебры, цифровой обработки сигналов, операционного исчисления и теории арифметического кодирования информации
Награды и премии	

Вильжан Мавлютинович Амербаев (25 апреля 1931 — 14 декабря 2014[1]) — советский, казахстанский и российский математик, академик АН Казахской ССР (1987).

Содержание

Биография

В 1954 году закончил КазГУ им. С. М. Кирова (Алма-Ата) по специальности «математика». С 1959 года — аспирант Математического института им. В. А. Стеклова АН СССР. Защитил кандидатскую диссертацию на соискание учёной степени кандидата физико-математических наук на учёном совете МИАН СССР в 1963 году. Тема диссертации — «Численные методы обращения интегрального преобразования Лапласа».

В 1959–1963 гг. — младший научный сотрудник, заведующий лабораторией вычислительной и машинной математики при президиуме АН КазССР.

В 1967–1972 гг. — заведующий отделом специализированного вычислительного центра МЭП СССР.

В 1972–1978 гг. — заместитель директора Института математики и механики АН КазССР.

В 1978–1989 гг. — заведующий кафедрой электронно-вычислительных машин МИЭТ.

В 1988–1993 гг. — академик-секретарь отделения физико-математических наук АН РК, член президиума АН РК.

С 1994 г. ведущий научный сотрудник Института теоретической и прикладной математики НАН РК.

В 1994–2002 гг. — профессор кафедры высшей математики в МИЭТ.

В 2002–2007 гг. — главный научный сотрудник ГУП НПИ «СПУРТ».

В 2007–2014 гг. — главный научный сотрудник ИППМ РАН.

Доктор физико-математических наук (1971), профессор (1973), член-корреспондент АН Казахской ССР (с 1972), академик НАН РК (1989).

Награды и премии

- Медаль за доблестный труд в ознаменование 100-летия со дня рождения В. И. Ленина (1970 г.)
- Медаль «За трудовую доблесть» (1971 г.)
- Лауреат Государственной премии СССР по науке и технике (1991 г.)

Характеристика трудов

Его труды относятся к операционному исчислению и теории арифметического кодирования информации. Его математическая активность в области информатики связана с привлечением фундаментальных алгебраических структур для организации вычислений в целях достижения высоких показателей по быстродействию, надёжности, точности на вычислительных средах специального назначения, повышения качества приборов (измерений) и сжатия визуальной информации. Основные

результаты — теория модулярного кодирования в кольце главных идеалов, цифровые методы отображения интегралов Лапласа, обобщённое операционное исчисление, новые и численные методы деконволюции. Выполнил большой цикл работ в области компьютерной алгебры и цифровых методов обработки сигналов. Результаты исследований отражены в более чем 100 печатных работах и заявках на изобретения, в том числе в 6 монографиях.

Монографии

- Акушский И. Я., Пак И. Т., Амербаев В. М. Основы машинной арифметики комплексных чисел. — Алма-Ата: Наука, 1970. — 248 с.
- Обобщенные ряды Лагерра и операционное исчисление. — Алма-Ата: Наука, 1974. — 181 с.
- Теоретические основы машинной арифметики. — Алма-Ата: Наука, 1976. — 323 с.
- Распределение регулярных потоков сообщений в информационных системах. — Алма-Ата: Наука, 1980. — 143 с.
- Параллельные вычисления в комплексной плоскости. — Алма-Ата: Наука, 1984. — 177 с.
- Анализ и синтез лагеррованного спектра. — Алма-Ата: Наука, 1984. — 180 с.

Ссылки

- Амербаев Вильжан Мавлютинович
- Амербаев Вильжан Мавлютинович на сайте «Жизнь замечательных людей Казахстана»

Опубликовано на сайте

— • —

Известия Академии наук КазССР, серия физико-математическая
3 (160), май-июнь 1991,
Алма-Ата, Гылым. — С. 90–91.

Юбилейные даты

Известия АН КазССР.
Серия физико-математическая, 1991, № 3

ВИЛЬЖАН МАВЛЮТИНОВИЧ АМЕРБАЕВ
(К 60-летию со дня рождения)

Исполнилось 60 лет со дня рождения и 37 лет научно-организационной, педагогической и общественной деятельности доктора технических наук, профессора, академика-секретаря Отделения физико-математических наук АН КазССР, академика АН КазССР Вильжана Мавлютиновича Амербаева.

В. М. Амербаев родился 25 апреля 1931 г. в г. Талды-Кургане. После окончания Казахского государственного университета им. С. М. Кирова в 1954 г. он работал до 1956 г. на механико-математическом факультете в должности ассистента. В 1959 г. после окончания аспирантуры при Математическом институте АН СССР и защиты кандидатской диссертации он трудился в секторе математики и механики АН КазССР вначале младшим научным сотрудником, а с 1962 г. заведующим лабораторией машинной и вычислительной математики. С 1962 г. В. М. Амербаев работал в Москве заведующим отдела Специализированного вычислительного центра. В 1971 г. он защитил докторскую диссертацию, а в 1972 г. был назначен заместителем директора Института математики и механики АН КазССР и избран членом-корреспондентом АН КазССР. С 1976 г. Вильжан Мавлютинович заведовал кафедрой Московского института инженеров гражданской авиации, затем он — профессор Московского института электронной техники и научный консультант Научного центра по электронной технике. С 1988 г. В. М. Амербаев работал в АН КазССР заведующим лабораторией Института математики и механики, в том же году он был избран академиком-секретарем Отделения физико-математических наук АН КазССР, а в 1989 г. — академиком АН КазССР.

В. М. Амербаев внес большой вклад в развитие вычислительной математики. Широкую известность получили разработанные им новые численные методы обращения интегральных преобразований Лапласа и Фурье. Он является большим специалистом в области разработки арифметических основ современных вычислительных машин. Его теория арифметического кодирования в кольце главных идеалов и методы организации компьютерных вычислений представляют собой весомый вклад в науку. Крупные результаты, имеющие важное народнохозяйственное значение, получены им в области цифровой обработки сигналов — предложены алгоритмические методы повышения разрешающей способности средств дистанционного зондирования при фиксированных технологических ограничениях.

В. М. Амербаевым опубликовано более 90 научных трудов, из них 6 монографий. Он имеет 20 авторских свидетельств на изобретения. В. М. Амербаев уделяет много внимания подготовке высококвалифицированных научных кадров. В числе его учеников три доктора и двадцать три кандидата наук.

Научно-организационную работу В. М. Амербаев успешно совмещает с обществен-

ной. Он — председатель комиссии при Президиуме АН КазССР по космическим исследованиям, сопредседатель совета по автоматизации научных исследований при Президиуме АН КазССР, председатель рабочей группы по информатизации республики, председатель проблемного совета по информатике, заместитель главного редактора журнала «Известия АН КазССР. Серия физико-математическая».

Научные заслуги В. М. Амербаева отмечены медалями «За трудовую доблесть», «За доблестный труд в ознаменование 100-летия со дня рождения В. И. Ленина» и Грамотой Верховного Совета КазССР.

Редакционная коллегия журнала сердечно поздравляет Вильжана Мавлютиновича со славным юбилеем и желает ему доброго здоровья, новых творческих успехов в научной и научно-организационной работе.

— • —

Журнал «Изобретатель и рационализатор»

Федеральный научно-популярный журнал «Изобретатель и рационализатор» проводит ежегодный конкурс «Техника — колесница прогресса» с вручением диплома и медали.

По итогам конкурса 2007 г. его лауреатом стал Вильжан Мавлютинович Амербаев.

В первом номере журнала были подведены итоги конкурса и опубликована статья заместителя главного редактора журнала В. Т. Бородина, ранее аспиранта В. М. Амербаева.

КР №1/2008

Лауреаты конкурса КР «ТЕХНИКА —

АМЕРБАЕВ Вильжан Мавлютинович

Москву, что было тогда великой честью. И хотя В.Амербаев был уже зав. лабораторией, получил квартиру, у него была семья, он поехал. В Зеленоград. Здесь решалась часть задачи противоракетной обороны, а именно — создание быстродействующей ЭВМ для управления системами многоканальных стрельбовых комплексов.

Работал большой коллектив. Сразу включившись, Вильжан Мавлютинович познакомился с ребятами, занимавшимися техническими проблемами МА, написал серьезный проект по МА. Возник взаимный интерес. Разработка алгоритмов и их аппаратная реализация велись одновременно. «Ночью Вильжан Мавлютинович думает, утром результаты передают схемотехникам. Аппаратную реализацию нового варианта с новыми вопросами показывают Амербаеву, он опять уходит думать. И так, пока его идеи не будут хорошо аппаратно реализованы». Патентова-

кольце главных идеалов. Через два года В.Амербаев снова в Алма-Ате, работает зам. директора Института математики АН КазССР, проповедует идеологию модулярности. В 1978 г. возвращается в Москву и работает сначала в МИИГА, а затем в МИЭТе. Студенты последнего вспоминают, что это было нелегкой задачей — изучать высшую математику у профессора Амербаева. В 1987 г. он был избран академиком и проработал академиком-секретарем отделения физ.-мат. наук Академии наук Казахстана до 1993 г.

С распадом Союза интерес к математике резко упал и востребованной оказалась криптография. Сейчас В.Амербаев сочетает МА с криптографией, в которой проблемы сложности и стойкости алгоритмов — это математические проблемы.

Ныне наступил период, когда создаваемые интегральные системы (ИС) содержат миллиарды элементов. Из-за этого их надежность может упасть. Повышение

Амербаев Вильжан Мавлютинович

Отец нашего лауреата преподавал математику в алма-атинском пединституте. Много позднее учился в Математическом институте им. В. А. Стеклова в Москве. Но чистый математик из Вильжана Мавлютиновича, считает он, не получился. «Виноват» в этом его руководитель В. А. Диткин, который сам из теоретической математики перешёл к прикладной. Первая большая работа В. Амербаева «Численные методы обращения интегральных преобразований» стала основой его кандидатской диссертации.

В 1965 г. в Алма-Ату приехали И. Я. Акушский и Д. И. Юдицкий, которые познакомили с новым направлением — модулярной арифметикой (МА). Поставили несколько задач. Одна задача показалась Вильжану Амербаеву близкой к интерполяционным проблемам, и, просидев ночь, на следующий день он показал своё понимание поставленных задач. Давлет Юдицкий, увидя это, предложил поехать работать в Москву, что было тогда великой честью. И хотя В. Амербаев был уже завлабораторией, получил квартиру, была семья, он поехал, в Зеленоград. Здесь решались задачи противоракетной обороны, а именно создание быстродействующей ЭВМ для управления системами многоканальных стрельбовых комплексов.

Работал большой коллектив. Сразу включившись, Вильжан Мавлютинович познакомился с ребятами, занимавшимися техническими проблемами МА, написал серьёзный проект по МА. Возник взаимный интерес. Разработка алгоритмов и их аппаратная реализация велись одновременно. «Ночью Вильжан Мавлютинович думает, утром результаты передают схемотехникам. Аппаратную реализацию нового варианта с новыми вопросами показывают Амербаеву, он опять уходит думать. И так, пока его идеи не будут хорошо аппаратно реализованы». Патентовались окончательные решения — главным было выполнить задачу. В. Амербаев пришёл к пониманию, что МА можно реализовать в кольце главных идеалов. Получилось довольно много разных модулярных конструкций.

Противник считал, что надо ударить по Москве, а все остальное само развяжется. Планировалось нападение сотней боевых ракет, каждая из которых при подходе к цели выпускает десять ложных. Надо было вычислить в этой армаде, какие ракеты реальные, и вести стрельбу по ним. Распознавание — в основном по траекториям. Задача сложная, потребовались массовые параллельные вычисления, большие скорости. Сделали ЭВМ с быстродействием 1 млн 200 тыс. операций, а лучшие в то время не работали быстрее 20000 оп/с.

В 1971 г. Вильжан Мавлютинович защитил докторскую диссертацию по применению в вычислительной технике МА в кольце главных идеалов. Через два года В. Амербаев снова в Алма-Ате, работает замдиректора Института математики АН КазССР, проповедует идеологию модулярности. В 1978 г. возвращается в Москву и работает сначала в МИИГА, а затем в МИЭТе. Студенты последнего вспоминают, что это было нелёгкой задачей — изучать высшую математику у профессора Амербаева. В 1987 г. он был избран академиком и проработал академиком-секретарём отделения физ.-мат. наук Академии наук Казахстана до 1993 г.

С распадом Союза интерес к математике резко упал и востребованной оказалась криптография. Сейчас В. Амербаев

сочетает МА с криптографией, в которой проблемы сложности и стойкости алгоритмов — это математические проблемы.

Ныне наступил период, когда создаваемые интегральные системы (ИС) содержат миллиарды элементов. Из-за этого их надёжность может упасть. Повышение надёжности ведёт к удорожанию интегральных схем. Возникла идея увеличения надёжности на уровне вычислений, возвращающая к использованию МА — единственной структуры, обладающей свойством самокоррекции. С другой стороны, отечественная микроэлектроника может повысить скорость и надёжность за счёт применения МА.

Вильжан Амербаев считает, что модульные операции можно ускорить, выполняя их по-другому, стандартизировать и приблизиться к двоичным технологиям. В этом его поддерживает директор Института проблем проектирования в микроэлектронике академик РАН А. Л. Стемпковский, заметивший, что «в МА есть замечательные штучки, я чувствую это». Вильжан Мавлютинович — автор двух десятков изобретений, более сотни статей, нескольких монографий, академик НАН Республики Казахстан, лауреат Государственной премии СССР, один из корифеев модулярной арифметики.

В. Бородин

— • —

Портал «Зеленоград.ру»

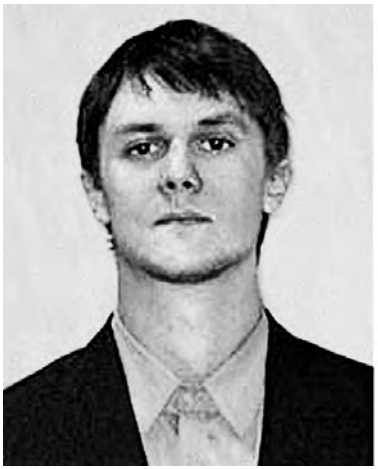
https://www.zelenograd.ru

Благодарные ученики о В. М. Амербаеве

https://www.zelenograd.ru/news/38851/
01.03.2016

Академия наук наградила зеленоградских учёных за применение модулярной арифметики в микроэлектронике

Екатерина Балака и Дмитрий Тельпухов, молодые специалисты зеленоградского Института проблем проектирования в микроэлектронике РАН, получили медали и денежные премии в 50 тысяч рублей за исследование в области информатики, вычислительной техники и автоматизации. Свою награду они посвятили памяти своего наставника, крупного учёного-математика Вильжана Амербаева[1].



Дмитрий Тельпухов и Екатерина Балака

[1] Кстати, именно аспиранты Д. Тельпухов и Е. Балака записали произнесённое в беседе высказывание своего научного руководителя В. М. Амербаева о математике, приведённое в начале настоящего сборника.

Президиум РАН по итогам конкурса 2015 года наградил молодых учёных ИППМ РАН за научно-исследовательскую работу «Разработка микроэлектронных устройств цифровой обработки сигналов с применением математического аппарата системы остаточных классов», как сообщила Российская академия наук.

Модулярная арифметика вместо двоичной системы

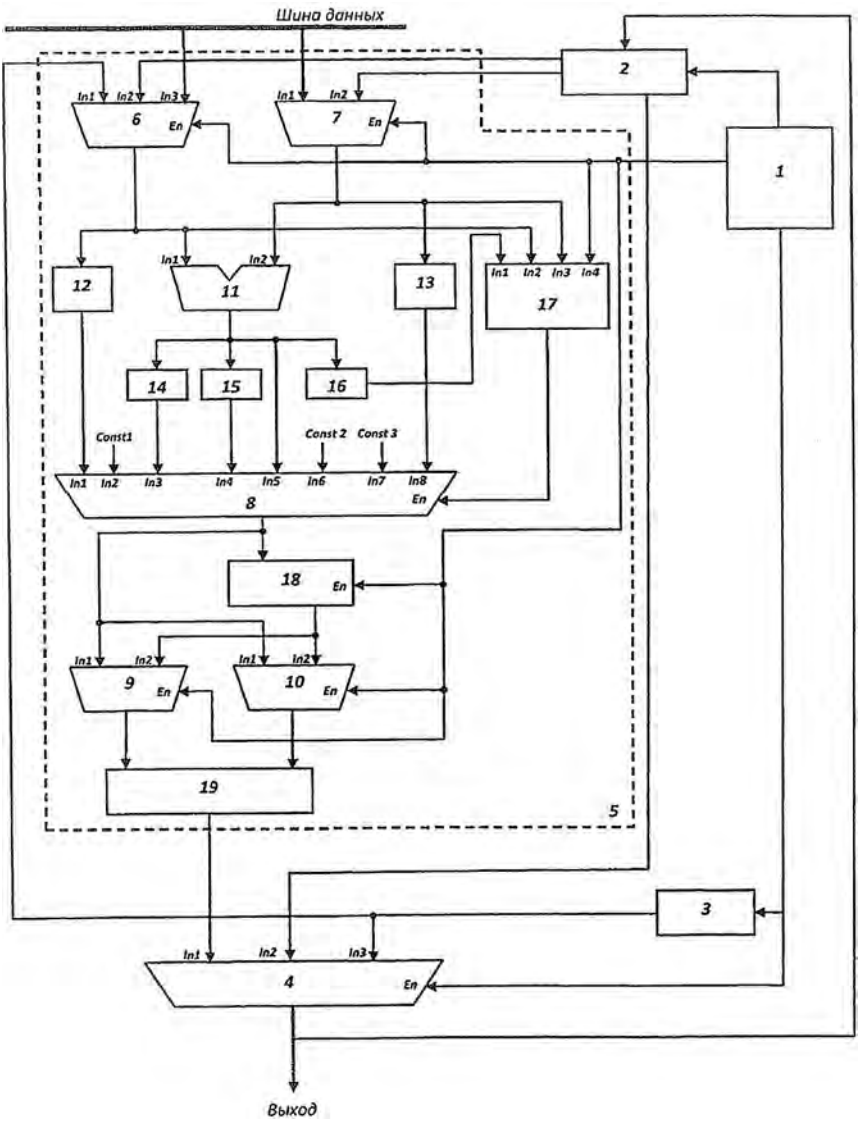
Суть исследования Zelenograd.ru пояснил Дмитрий Тельпухов, кандидат технических наук, заведующий отделом методологии проектирования интегральных схем ИППМ РАН: «В настоящее время все вычислительные средства выполнены на двоичных технологиях, где всё считается в двоичной системе (нули и единицы), а мы использовали систему остаточных классов, где гораздо больше диапазон и, соответственно, больше возможностей параллелизма для вычислений. По сути, этим мы значительно повысили вычислительную мощность устройств».

По мнению молодого учёного, результаты исследования, патент на которое был получен в 2014 году, можно применить в обычных компьютерах и в суперкомпьютерах, но в ограниченном спектре задач — так, модулярная арифметика с применением остаточных классов может ускорить процессы, в которых много арифметических вычислений.

«На текущей элементной базе, используя такую систему счисления и различные дополнительные методы, можно распараллелить вычисления и решать быстрее определённый класс задач», — отметил он.

В отличие от денежной премии Правительства Москвы, недавно присуждённой за наукоёмкие разработки молодым ученым МИЭТа, медаль РАН в ИППМ воспринимают как академическую награду, признание заслуг молодёжи.

Дмитрий Тельпухов заявил, что они хотели бы посвятить награду своему научному руководителю профессору Амербаеву, родоначальнику направления модулярной арифметики, который ушёл из жизни в прошлом году.



Вычислительный элемент бимодульной модулярной арифметики — описанная в патенте полезная модель с устройством управления, ОЗУ, ПЗУ и мультиплексором, в состав которой введён специальный арифметический узел (схема его работы)

«Мы пытаемся нести его флаг»

Амербаев Вильжан Мавлютинович

«Наш отдел методологии проектирования интегральных схем существует в институте довольно давно, модулярной арифметикой мы занимаемся лет семь», — рассказал учёный Zelenograd.ru. — «Огромный вклад в развитие этого направления в России, да и во всём мире, внёс Вильжан Мавлютинович Амербаев, его перу принадлежит много трудов и монографий, получивших международное признание. Мы пытаемся нести его флаг дальше и по мере сил развивать идеи, заложенные им ещё в пятидесятые годы.

Я сам попал в институт благодаря Амербаеву. Поначалу он был моим руководителем практики на предприятии, которую я проходил в компании «АНКАД». Он заинтересовал меня модулярной арифметикой и предложил перейти на работу в институт. С тех пор я тут и работаю. Был стажёром, потом исследователем, потом младшим научным сотрудником и так постепенно дорос до заведующего отделом. У нас молодой отдел — больше 50% молодых учёных: аспиранты, студенты проходят практику. Это политика института, наш директор очень поощряет молодёжь, потому что это рабочие руки и новые идеи».

Дмитрий Тельпухов родился в 1986 году, закончил в 2009 году МИЭТ, факультет «Микроприборы и техническая кибернетика». Автор и соавтор более 30 научных работ. Екатерина Балака — кандидат технических наук, старший научный сотрудник отдела методологии проектирования интегральных схем ИППМ РАН. Родилась в 1987 году, закончила тот же факультет МИЭТа в 2010 году, также является автором и соавтором более 30 научных работ. Область научных интересов

обоих — схемотехника и проектирование цифровых схем, цифровая обработка сигналов, модулярные вычислительные структуры.

ИППМ РАН создан в Зеленограде в 1986 году для выполнения фундаментальных научных исследований и прикладных разработок в области проектирования нано- и микроэлектронных систем и устройств. В числе сотрудников — два члена РАН, восемь докторов наук и 16 кандидатов наук.

Вильжан Мавлютинович Амербаев был главным научным сотрудником института с 2007 года, совмещая научную деятельность с работой на кафедре вычислительной техники МИЭТ. Российский и казахский математик, доктор технических наук (1971 год), профессор вычислительной математики, академик Национальной академии наук Казахстана. В 1991 году он стал лауреатом Государственной премии СССР по науке и технике. Также был ведущим научным сотрудником зеленоградского НПЦ «СПУРТ» и главным специалистом зеленоградской фирмы «АНКАД». Сфера научных интересов — проблемы обращения интегральных преобразований, защита информации методами кодирования, цифровая обработка. Читал курсы «Высшая математика» и «Математические основы защиты информации».

ГЛАВА 5

БЛИЗКИЕ, ДРУЗЬЯ, КОЛЛЕГИ И УЧЕНИКИ О В. М. АМЕРБАЕВЕ

В этой главе представлены воспоминания о Вильжане Мавлютиновиче Амербаеве его близких, друзей, коллег по работе и учеников, дополнительно свидетельствующие о его уникальных профессиональных, культурных и человеческих качествах.

Воспоминания расположены в алфавитном порядке авторов.

Все воспоминания подготовлены авторами для настоящего сборника.

СВЦ-шники Малашевич Б. М., Рахмина Г. В., Амербаев В. М. и журналистка зеленоградской газеты, 22.09.2011, Зеленоград

Гордость казахстанской и российской математики

Акназарова Р. Б., к.ф-м.н., зам. директора Департамента дистанционного зондирования Земли АО «Национальный центр космических исследований и технологий»

Акназарова Раушан Булатовна

Впервые я услышала о Вильжане Мавлютиновиче Амербаеве от своего дяди Хаиржанова Рашида Гафаровича, который в 1960-е годы работал в Институте математики и механики Академии наук Казахской ССР. В целях подготовки высококвалифицированных научных кадров институт традиционно направлял молодых специалистов в ведущие научные центры Москвы, Новосибирска, Киева, Ленинграда на стажировку и обучение в аспирантуре.

Дядя Рашид в числе группы молодых учёных обучался в аспирантуре Института кибернетики Академии наук Украинской ССР в Киеве. В то время я училась в школе и с огромным интересом слушала рассказы дяди о новых направлениях в прикладной математике, электронных вычислительных машинах, новых задачах в области кибернетики, об институте кибернетики, о Киеве и его достопримечательностях.

С особым уважением дядя рассказывал о руководителях и ведущих учёных Института математики и механики — академиках Персидском К. П., Жаутыкове О. А., Тайманове А. Д., Ержанове Ж. С., Амербаеве В. М., Паке И. Т. У него, как у молодого учёного, занимающегося проблемами кибернетики, особенный интерес вызывали научные результаты Вильжана Мавлютиновича Амербаева.

В то время Амербаев В. М., закончив аспирантуру Математического института им. В. А. Стеклова и защитив кандидатскую диссертацию, был уже известным учёным в области машинной арифметики, теории арифметического кодирования информации, параллельных вычислений. Получив прекрасные знания в России — в научной школе академика А. А. Дородницына и профессора В. А. Диткина, а в Казахстане — в школе академика К. П. Персидского, Амербаев В. М. создал свою школу, получившую широкое признание научной общественности.

Любовь к математике передалась от дяди и ко мне: окончив школу № 56 с физико-математическим уклоном, затем — механико-математический факультет Казахского государственного университета им. С. М. Кирова, я с 1978 года начала работать в Институте математики и механики.

Институт в то время возглавлял Умирзак Махмутович Султангазин, руководивший им с 1978 по 1989 годы и внёсший весомый вклад в развитие теоретической и прикладной математики в Казахстане. Под руководством академика У. М. Султангазина Институт математики и механики в те годы представлял собой крупный научный центр с актуальными направлениями в области математики, механики, вычислительной и прикладной математики. Работы многих сотрудников института были признаны мировой научной общественностью, а коллективный труд института неоднократно отмечался переходящим знаменем в социалистическом соревновании. Международные конференции, проводимые институтом, и научные форумы в зарубежных странах, в которых принимали участие учёные института, подтверждали высокий уровень и востребованность выполняемых исследований. Результаты фундаментальных и прикладных исследований института в области математики и механики воплощались в монографии, статьи в известных зарубежных и советских научных изданиях. В те годы под руководством Султангазина У. М. и Пака И. Т. был организован вычислительный центр коллективного пользования для всех академических институтов. По своим научным достижениям Институт математики и механики в тот период был одним из лучших научных институтов в стране.

Хотя Вильжан Мавлютинович уже уехал работать в Москву, его присутствие в институте чувствовалось долгое время: в рассказах старших коллег сквозило уважение и тёплое отношение к нему, чувствовался его высокий авторитет в коллективе. С особенным чувством уважения и признательности относился к Амербаеву В. М. заместитель директора института Пак Иван Тимофеевич, который сохранил это отношение и до настоящего времени!

В 1988 году Вильжан Мавлютинович вернулся в Алма-Ату в связи с назначением на должность академика-секретаря отделения физико-математических наук академии наук РК, где он работал до 1993 года, являясь и членом президиума Академии наук Республики Казахстан.

За эти годы отделение стало одним из ведущих подразделений академии наук. В составе отделения находились девять крупных институтов физико-математического направления: Институт ядерной физики, Физико-технический институт, Институт физики высоких энергий, Астрофизический институт им. В. Г. Фесенкова, Институт ионосферы, Институт математики и три новых института, которые в 1991 году были образованы на базе Института математики и механики — Институт космических исследований, Институт проблем информатики и управления, Институт механики и машиноведения. Это были нелёгкие годы перестройки, становления независимости государства. Казахстанская наука также переживала непростые времена: проблемы с финансированием, оснащением материально-технической базы институтов, кадровым обеспечением.

Мудрая дальновидная политика, проводимая академиком-секретарём отделения физико-математических наук Амербаевым В. М., способствовала успешному развитию научно-организационной деятельности всех институтов отделения, эффективной реализации выполняемых программ фундаментальных и прикладных исследований, сохранению и укреплению научно-технического потенциала институтов. Чтобы руководить таким неоднородным по научным направлениям и кадровому составу объединением научных организаций, необходимо было иметь особый дар лидера, признанного авторитетного учёного

и, что наиболее важно, уметь создать команду единомышленников, владея талантом общения с коллегами. И всеми этими качествами сполна обладал Вильжан Мавлютинович! Его интеллигентность, тактичность, способность услышать собеседника, понять его проблемы и найти нужные слова поддержки вызывали искреннее уважение и признание.

Мне посчастливилось в те годы работать рядом с Вильжаном Мавлютиновичем, непосредственно под его руководством в рамках отделения физико-математических наук. Наш Институт космических исследований, основателем и первым директором которого был академик Султангазин У. М., входил в состав отделения. Профессор Закарин Э. А. работал в должности заместителя директора по науке, я — в должности учёного секретаря института. Я благодарна судьбе, что в то время мне, ещё новичку в административной сфере научно-организационной деятельности, была предоставлена возможность работать рядом с такими крупными учёными и талантливыми организаторами науки. Это была настоящая школа!

Вильжан Мавлютинович одинаково уважительно относился и к академикам, и к рядовым научным сотрудникам. Как требовательно и в то же время дипломатично он проводил заседания бюро отделения, на которых рассматривались и обсуждались злободневные вопросы текущей деятельности и актуальные задачи перспективных научных исследований! На заседаниях всегда были оживлённые горячие дискуссии руководителей и ведущих учёных всех институтов отделения, иногда доходящие до жарких споров. Но под руководством Вильжана Мавлютиновича в конце заседания всегда принималось единственное правильное конструктивное решение, причём поддерживаемое единогласно всеми участниками дискуссий.

К нам, молодым учёным, Вильжан Мавлютинович относился с особой теплотой, по-отечески. При беседах он не ограничивался только официальной стороной разговора, а интересовался и общечеловеческими гранями жизни: увлечениями, интересами, настроением, здоровьем, личными проблемами! Он в каждом из нас видел коллегу, соратника, единомышленника. И мы очень дорожили этими отношениями.

При встречах он очень внимательно беседовал, вникая в суть ежедневных проблем и текущих задач научно-организационной деятельности каждого института. А институты нашего отделения были в то время крупными научными центрами со своей сложной инфраструктурой и солидным штатом научных и инженерно-технических работников.

В. М. Амербаев, Р. Б. Акназарова и Е. Е. Ергожин, 1996 г.

В жизни Вильжан Мавлютинович был очень деликатным, отзывчивым, высокоинтеллигентным, светлой и чистой души человеком! В моей памяти надолго сохранятся его добрые глаза, улыбчивое лицо, галантность и величавая осанка, тёплое и уважительное отношение! Когда он приезжал в Алматы в последние годы, мы все с бесконечным уважением и восхищением радовались встречам с ним, словно возвращались в ту замечательную эпоху классической академической действительности.

Светлая память о Вильжане Мавлютиновиче Амербаеве всегда будет в наших сердцах... Здоровья, счастья, успехов, благополучия всем его родным и близким, коллегам, ученикам!

Вильжан во всем был прост, как Правда

Амирбаева Л. М.,
сестра

Амирбаева Лейла
Мавлитдиновна

Мои родители родом из города Талды-Курган. Мать Чинибекова Ашраф Ризаевна (29.12.1910 — 30.01.1991) родилась в семье богатого купца Ризы. Отец Амирбаев Мавлитдин Оспанович (16.04.1908 — 16.10.1987) родился в семье ремесленника (портного).

Отец папин Оспан работал батраком у маминого отца. Молодые мама и папа полюбили друг друга. В те времена пожениться им бы никто не разрешил. Они убежали из дома тайком и уехали в Алма-Ату, не взяв с собой ничего. Это было в 1926 году. Помог им устроить этот побег и сам сбежал вместе с ними Канабек Байсеитов, в дальнейшем известный казахский актёр. В те времена в г. Талды-Кургане он работал милиционером. Потом он женился на певице Куляш. Её называли соловьём казахского народа. Так началась у моих родителей самостоятельная жизнь в Алма-Ате.

Мама и папа, как и многие в то время, получили образование на рабфаках (рабочие факультеты). В 1932 году папа закончил обучение в первом в Алма-Ате вузе — педагогическом институте по специальности «*математик*». И там же начал работать преподавателем.

Папа был в числе тех молодых людей, которые взяли на себя миссию поднять образование в молодой советской республике Казахстан, дать образование казахскому народу.

Как преподавателю вуза, ему и его молодой семье дали в общежитии преподавателей комнату. Потом родился у них сын. Папа, воодушевлённый идеями революции и преданный советской власти, назвал сына ВИЛИК, т. е. Владимир Ильич Ленин и Крупская. Но малышу не суждено было долго жить. Мама приняла это как кару за то, что она ослушалась родителей, сбежав с папой в Алма-Ату. И второго ребёнка мама уехала рожать в Талды-Курган, к родителям. Так 25 апреля 1931 года родился Вильжан.

Но дедушка Оспан при оформлении документов Вильжана перепутал некоторые буквы в фамилии (Амербаев, вместо Амирбаев) и в отчестве (Мавлютинович, вместо Мавлитдинович). Так возникло это несовпадение с документами других детей.

Когда началась Великая Отечественная война, папа работал в Казахском государственном университете (КазГУ). На фронт он уехал в 1942 году по зову долга и чести (отказался от брони, которую имел как преподаватель вуза). Тогда в семье было уже четверо детей: старший сын Вильжан — 11 лет, две дочери — 8 и 5 лет, и самая младшая я — 2,5 года. Маме удалось сохранить всех нас живыми и здоровыми и дождаться папу с фронта.

Папа воевал на Ленинградском и Прибалтийском фронтах. Был парторгом гвардейского миномётного полка. За мужество и отвагу в боях с фашистами награждён медалью «*За оборону Ленинграда*», орденами «*Красная Звезда*» и «*Отечественной войны 2 степени*» и многими другими наградами. Вернулся папа с фронта в ноябре 1945 года, т. к. после победы над Германией был направлен на Дальний Восток, где продолжалась война с японцами.

После войны он работал преподавателем математики в институтах нашего города: писал учебники по высшей математике, переводил их на казахский, внёс большой вклад в образование молодёжи. За свои труды он получил учёную степень кандидата физико-математических наук, звание доцента и награды «*Знак Почёта*», «*Заслуженный учитель Казахстана*» и др.

Мама и папа могли в семье всё так организовать, что мы всегда были сыты, спокойны и радостны. Мамиными заботливыми руками всегда была приготовлена вкусная еда. Большие праздники в стране мы всегда ждали с нетерпением, потому что мама всегда покупала нам заранее красивую одёжку и нам хотелось поскорее все надеть.

Потом в семье появились ещё два брата. Так у родителей в 1951 году было уже шестеро детей. Мы помогали маме. Каждый знал, кому что делать по дому без всяких указаний мамы. Она никогда детей не ругала, не наказывала за какие-то проступки, а просто спокойно беседовала, разъясняла. Таким образом, давала нам возможность самим осознать свои проступки, сделать правильные выводы.

Трудолюбие папы и мамы, доброта к людям, забота о детях, умение вести диалог с ними, понятие чести и совести — всё это повлияло на формирование характеров детей и послужило хорошим стержнем в организации личной жизни каждого: все получили высшее образование и создали благополучные семьи.

Вильжану часто приходилось работать в Алма-Ате. В этот период он жил у меня. По ночам работал и почему-то любил работать на кухне, хотя у него была отдельная комната с балконом на запад. Может быть потому, что на кухне был балкон с видом на восток: хорошо рано утром увидеть восход солнца, подышать прохладой, принять новый поток мыслей и творческих решений... А может, просто заниматься на кухне удобно: в любое время можно выпить глоток горячего бодрящего чая. Это были прекрасные времена, когда была возможность с ним общаться. В беседах он всегда умел слушать, никогда не спорил, и его совет был просто луч света и доброты в каких-то, казалось, тупиковых вопросах. Всё становилось ясно и так всё просто.

Как-то я спросила Вильжана: «*Как тебе удаётся так спокойно беседовать со всеми, кто бы к тебе ни обратился со всякими добрыми и недобрыми намерениями?*» Он коротко ответил: «*Надо научиться не давать волю своим раздражениям. Это сложно, но надо*».

Просто диву даёшься, сколько любви и добра в его душе к родным и самым дорогим ему внукам, детям, жене. Он всегда носил с собой фото своих внуков и дочерей. Часто вечерами сядет в кресло и рассматривает: вспоминает, тоскует. Но ясно одно: работа очень важна в его жизни. Утром бежит в академию. Всегда просто одет, постоянно аккуратный костюмчик, никаких такси-машин. Трамвай всегда довозил его до места работы. Шиковать было не по его нраву. Короче, во всем был прост, как Правда.

Иногда находили время в воскресные дни прогуляться по горным лесам, ущельям. Вильжан очень любил природу наших гор и восхищался, глядя на красоту их вершин, освещённых закатом багрового солнца: «*Ну, просто живые картины Рериха!...*» После такой прогулки чувствуешь прилив сил. От него всегда исходила позитивная энергия, какой-то положительный заряд. И здесь, в окружении природной красоты, какие-то мысли о творческой работе не покидали его. Он успевал делать записи в блокнотик, который всегда был в кармане.

Он очень преданно относился к своим друзьям, коллегам. Когда неожиданно умер его близкий друг Д. И. Юдицкий, он очень тяжело переживал эту потерю. Вот тогда и случился у Вильжана первый сердечный приступ. До конца своих дней он ощущал боль утраты матери — очень тяжело. Помню, когда мама умерла, я впервые в жизни слышала, как может рыдать в отчаянии взрослый мужчина. Он напомнил мне рёв медведя в клетке, когда я в детстве была в зоопарке и видела подобную сцену рёва.

И вот так тихо, совсем неожиданно он ушёл из жизни, чтобы никогда больше не ощущать боль утраты своих близких.

В последние годы Вильжан не часто приезжал в Алма-Ату. Только по каким-то событиям в академии наук. И когда он приезжал, это была для нас ликующая радость: собиралась вся близкая родня, застолье и обязательно зачитывался стих, посвящённый Вильжану в честь его приезда. Вот один из стихов к юбилею Вильжана:

Вильжан Мавлютинович, поздравляем!

Приятное событие есть в жизни людей,
Сегодня все празднуют твой юбилей!
Большой и широкий прошёл в жизни путь,
Есть что обсудить и по новой взглянуть.
Ты — старший в роду, ты сейчас корифей!
Все дело творят по указке твоей,
Тобой очень горд Амербаевский род,
Заслуги твои прославляет народ!
Для всех ты — пример, образец и маяк!
Высоко поднял Амербаевский стяг,
В Москве и по миру заслуги твои,
Все люди относят к заслугам Семьи.
Семья Амербаевых, Амербаевский род,
Все те, кто причастен, тобою он горд!
Живи много лет, плодотворно твори!
Свои назидания нам говори.
Пусть всё, что ты создал, сказал, написал,
Широкой Душой подарил и отдал,
К тебе возвращается щедрым добром,
Крепит тебя в жизни и греет Теплом!

2011
Жан и Бахыт Нургалиевы
Лейла Амирбаева

О моём учителе и наставнике

Бектасов А. Ж.,
сосед с детства и ученик

Где-то в середине 70-х годов 20-го века, когда я заканчивал обучение в вузе, (КазГУ, факультет прикладной математики), судьба наградила меня подарком и свела с членом-корреспондентом АН КазССР Амербаевым Вильжаном Мавлютиновичем — он стал научным руководителем моей дипломной

Бектасов Алихан Жилхайдарович

работы. Надо отметить, что я был не самым дисциплинированным и прилежным студентом, был не на лучшем счету и отношения с преподавательским составом у меня складывались непросто. Только на старших курсах я несколько остепенился, часть детской дури из меня постепенно выветрилась, и тут встреча и собеседование с Амербаевым! Сам уровень и форма собеседования, которое продолжалось минут 40–50, с уже известным в нашей студенческой среде именитым учёным сразу же произвели на меня впечатление. Как будто я оказался на Олимпе, а сам Зевс приоткрывает передо мной двери в храм науки и предлагает мне на секунду заглянуть туда и подержать в руке «*лавровый венок*». Т.е. уровень ответственности и доверия, которые возлагал на меня Вильжан Мавлютинович, предлагая быть его дипломником, я ощутил сразу. В результате я совершенно изменил своё отношение к учёбе, к дисциплине, а дипломную работу под руководством В. М. Амербаева защитил уже на *отлично*. И почти сразу он предложил мне дальнейшую работу у него в Институте математики и механики Академии наук КазССР, где он являлся на тот момент заместителем директора. Для меня это было честью, о таком я даже не мечтал, естественно, сразу согласился и сказал ему об этом.

Буквально через несколько дней из академии наук поступил запрос о моём направлении туда как молодого специалиста.

Однако я очень скоро получил от жизни новый урок, например, что наука — это не только интересные исследования и открытия, но и, как все сферы человеческой деятельности, это ещё и терпение, тяжёлый труд, а также борьба, интриги, заговоры, обман и пр. Оказалось, что декан моего факультета, с которым у меня и так были не самые лучшие отношения,

почему-то не шибко жалует Амербаева. Что было тому причиной — зависть, научные разногласия или ещё что, так и осталось неясным. Самому «*куснуть*» Амербаева или вступить с ним в открытый спор у него явно не хватало ни духу, ни знаний. Да и по статусу он явно был неровня члену-корреспонденту АН КазССР — ну, как денщик против генерала. Вот он и пытался выместить всё зло на студентах-выпускниках, у которых Амербаев был научным руководителем дипломных работ, а таких нас тогда было двое, я и ещё один мой сокурсник. Вот и решил, видимо, этот декан тогда «*завалить*» на защите дипломов нас обоих да ещё натравил на нас своих *лизоблюдов*, которые на защите буквально засыпали нас своими (в основном глупыми) вопросами. Правда, со мной у них ничего тогда не вышло, а вот моего сокурсника, который, в отличие от меня, практически все пять лет учился на «*отл.*», они всё же практически чуть не «*засыпали*», ему потом кое-как поставили *тройку* за дипломную работу. Более того, когда на меня пришёл запрос из АН КазССР о моём распределении туда, наш декан сделал всё, чтобы этот запрос не был удовлетворён. Он каким-то образом организовал моё распределение в одно из самых влиятельных и «*блатных*» министерств республики, мой запрос из академии наук и диплом об окончании вуза спрятал в сейфе одной из работниц канцелярии факультета, а сам взял отпуск и уехал куда-то на курорт. После этого началась моя более чем двухмесячная эпопея по поиску запроса и диплома, а также получения открепления от того министерства, куда меня этот декан «*сосватал*».

Вот тут Вильжан Мавлютинович, показал мне своим личным примером, каким должен быть настоящий руководитель и учёный! Он не стал размениваться на какую-то возню или борьбу с тем, кто того не достоин, не стал тратить на него своё время. Он просто проявил свою выдержку и достоинство и от своего решения и слов не отказался. Другой бы на его месте мог просто не ждать моего выхода на работу и взял бы на эту вакансию кого-либо другого, не такой уж важный и незаменимый специалист я был, особенно на тот момент. Но во время

одной из наших встреч, когда я докладывал ему о своих трудностях с поиском своего диплома и других документов, Вильжан Мавлютинович лишь слегка покачал головой и совершенно спокойно и уверенно сказал мне примерно так: «*Ничего, давай подождём, а ты пока продолжай заниматься поиском и оформлением документов. «Собака лает, а караван идёт!», вот и мы будем двигаться дальше...*» В итоге все мои вопросы так или иначе решились положительно, и свою трудовую деятельность я начал уже в качестве довольно лаборанта лаборатории проблем оптимального кодирования ИММ АН КазССР под непосредственным началом Вильжана Мавлютиновича.

Причём кроме меня в этой лаборатории оказалось ещё несколько таких же молодых специалистов, недавних выпускников вузов, с которыми мы, естественно, сдружились и в дальнейшем рабочее и нерабочее время проводили вместе, споря и обсуждая наши научные изыскания. Некоторые за глаза даже называли нас «*птенцы Амербаева*» или «*битгруппа Амербаева*», и мы этим даже гордились. Особых привилегий, тем более финансовых, это нам не давало, но определённый гонор всё же прибавляло, и мы смело, особенно на научных семинарах и конференциях, вступали в дискуссии и научные споры с более старшими и именитыми сотрудниками института. Нередко делали это группой, поддерживали друг друга. И тут уже прежние заслуги и научные звания наших оппонентов не позволяли им игнорировать и пресекать наши каверзные вопросы и сомнения. Но дело от этого только выигрывало, в обстановке такой демократии и спорах действительно рождалась истина!

Что ещё меня поражало и восхищало в Амербаеве, так это стиль его руководства, выдержка и спокойствие в любой ситуации. Никогда не видел и не слышал, чтобы он на кого-то повышал голос, даже если те того и заслуживали. Он никогда не унижал и не угрожал своим подчинённым. Коллектив ИММ АН КазССР был довольно значительным по численности, а там, где много людей, нередко возникают различные сложные жизненные ситуации — на работе, дома, на улице и т. д. Бывали случаи

различных ЧП, даже в таком научном учреждении. В некоторых случаях могли обвинить и Амербаева как руководителя за недосмотр и халатность. Другой на его месте стал бы орать на виновных, наказал их или даже избавился от них. Но только не Вильжан Мавлютинович, который всегда поступал справедливо и по-человечески, но в то же время всегда только в соответствии с законом. За это сотрудники его любили и уважали.

Что ещё мне запомнилось? Что он никогда не тратил время на пустые развлечения, не было у него так называемого хобби. Ни разу не видел, чтобы он играл в шахматы, в шашки, в карты и т. п., хотя в научных учреждениях многие занимаются таким времяпровождением.

Для меня именно этот пример знаменателен тем, что Вильжан Мавлютинович был всегда тем идеалом, которому хочется подражать и на которого хочется быть похожим. Признаюсь, что как ни старался, это мне не всегда и не во всём удавалось. Возможно, мы по характеру и темпераменту были всё же разные. Например, у меня всегда был темпераментный и взрывной характер, потом я, правда, довольно быстро «*отходил*» и нередко сожалел о содеянном. Но такой выдержки и сдержанности, как у Амербаева, так и не достиг. А в данном случае, насчёт азарта и хобби, у меня получилось, и за всю свою последующую жизнь я практически не играл и не пристрастился ни к шахматам, ни к картам, ни к какой другой игре, в том числе и к компьютерным играм. У меня всегда перед глазами стоял пример Вильжана Мавлютиновича. А именно один случай. Как-то в конце обеденного перерыва он пришёл с обеда чуть раньше обычного и застал момент, когда во время перерыва несколько наших сотрудников играли в шахматы, причём один из них, даже видя, как пришёл Амербаев, настолько обнаглел, что предложил ему сыграть с ним партию блиц в шахматы. На что Вильжан Мавлютдинович спокойно, уверенно, но несколько холодно сказал примерно следующее: «*Я вообще ни в какие игры принципиально не играю, так как считаю, что если человеку даны мозги и какие-то способности, то их надо применять по прямому назначению, а не использовать своё время и способности попусту для*

мастурбации мозгов. Поверьте, времени нам отпущено не так уж много, чтобы его разбазаривать». За всё время работы и общения с Вильжаном Мавлютиновичем это был единственный случай когда он ответил так резко. Но этот случай навсегда запал мне в память как руководство к обязательному исполнению...

Многие из нас, наверное, были свидетелями, когда на различных совещаниях, симпозиумах и т. п. на трибуне выступает докладчик, а слушатели в зале находятся как бы в другом пространственно-временном измерении. Кто-то дремлет, кто-то что-то читает, кто-то играет в *морской бой* или *крестики-нолики*. А все словесные и визуальные «*залпы*» докладчика улетают в пустоту. За многие века существования человечества было огромное количество так называемых учёных и ораторов. Но только немногие из них, по-настоящему великие, оставили свой след в истории, и именно благодаря тому, что умели так сформулировать и высказать свои мысли и результаты своих исследований, что они становились интересны и понятны многим, даже не очень образованным людям, что служило детонатором новых идей и исследований в достижении истины. Можно привести множество примеров такого утверждения. Вспомним хотя бы академиков отца и сына Капиц или знаменитого физика академика Иоффе и др., которые умели так объяснить свои сложнейшие научные открытия и изыскания, что заинтересовывали и убеждали многих. А в результате находили новых сторонников и талантливых учеников для продолжения и расширения своих исследований, для пропаганды науки.

Вот и в отношении Вильжана Мавлютиновича вспоминается такой случай.

Проходил научный семинар работников нашего института, а в зале (не в президиуме) присутствовал и В. М. Амербаев, хотя именно он являлся руководителем этого семинара. На трибуну вышел один из работников нашего института, кандидат наук, и стал выступать по своей тематике. Он буквально засыпал присутствующих потоком цифр, формул и специальных терминов. Мне никак не удавалось уловить и понять основную мысль и суть выступления, не возникало никакого интереса

к докладу. Было видно, что и многие из присутствовавших были в таком же состоянии, как и я. А встать и уйти нельзя. И тут неожиданно Вильжан Мавлютинович, который всегда отличался сдержанностью и деликатностью, встаёт, извиняется и прерывает докладчика примерно такими словами:

«*Простите, что прервал Вас, но, мне кажется, Вы несколько перегрузили свой доклад узкоспециальными терминами и формулами так, что сейчас даже я, вроде профессор, никак не могу вникнуть в суть Вашего выступления. А в зале не так много других профессоров, которые бы поняли Вашу тему. Потому давайте попробуем и начнём сначала, но только на простом человеческом языке. Я бы даже сказал «на крестьянском». И пожалуйста, особенно в начале выступления, поменьше формул...*». Докладчик, конечно, вначале растерялся, но потом всё же при поддержке и помощи Амербаева стал излагать свои мысли на простом «*крестьянском*» языке. И постепенно среди участников семинара появился интерес к докладу, глаза у них заблестели и стали задаваться первые робкие вопросы. А потом уже начались и какие-то дискуссии, к тому времени «*завёлся*» и сам докладчик. Начались споры, семинар оживился. В конце Амербаев подвёл итог и резюме к докладу, отметив, что если у кого-то появился интерес к теме и свои новые мысли, он может после семинара взять у докладчика копию письменного текста его выступления. «*Надеюсь, докладчик не пожадничает и поделится с желающими*» (смех в зале), — закончил Вильжан Мавлютинович. Кто-то решил поддержать его шутку и спросил: «*А к какому из докладчиков подойти?*» На что Амербаев ответил кратко: «*Докладчик у нас один (и указал ладонью в его сторону), а я простой переводчик на человеческий — «крестьянский» язык...*»

Потом тот докладчик так доработал свой доклад с учётом полученных замечаний и предложений, а также изложил его таким образом, что он даже был опубликован в одном из всесоюзных научных журналов.

В дальнейшем я не один раз слышал в институте этот термин — «*крестьянский*» язык, который некоторые даже переиначили: переходи на «*амербаевский*» язык!

Удивительно широко эрудированный, добрый и внимательный Человек

Бияшев Р. Г.,
коллега, друг

Бияшев Рустем Гакашевич

В 1973 г. по инициативе Вильжана Мавлютиновича мы с ним опубликовали статью «*Интерполяция и коды, исправляющие ошибки*». В этой статье предлагалось для обнаружения и исправления ошибок избыточность вводить с использованием интерполяционного полинома Лагранжа и коды, соответственно, назвать кодами Лагранжа.

Вообще первая половина 70-х прошлого века была не лучшим периодом в истории СВЦ — происходила вынужденная смена тематики с супер-ЭВМ на микропроцессоры и микро-ЭВМ. Поэтому некоторые сотрудники, даже из «старой гвардии», начали искать место своему лучшему применению. Одним из таких мест оказался открытый в 1971 году Всесоюзный НИИ проблем организации и управления ГКНТ СССР для разработки общегосударственой автоматизированной системы (ОГАС). Директором института был первый заместитель председателя ГКНТ Жимерин Д. Г., научным руководителем — академик Глушков В. М. В этот институт для разработки в рамках ОГАС общегосударственной системы передачи данных (ОГСПД) был приглашён в качестве начальника отдела работавший в СВЦ Черкасов Юрий Николаевич.

Поскольку в тот период средства компьютерной техники и каналов связи не отличались высокой надёжностью из-за довольно скромных показателей наработки на сбой и на отказ и ошибок при передаче данных, актуальными были разработки

теории кодирования (кодов, исправляющих ошибки или помехоустойчивого кодирования). Ю. Н. Черкасов каким-то образом прослышал про коды Лагранжа и про то, что к ним причастен В. М. Амербаев. А что касается репутации Вильжана, то всем было известно, что если он просто причастен к какому-либо делу, то это дело нужное и полезное, всё сделано правильно и чисто, всё обязано работать. Черкасов Ю. Н., например, однажды сказал так: «*Если ко мне с какой-либо просьбой обращается Вильжан, я бросаю все свои дела и стараюсь побыстрее выполнить его просьбу. Потому что все мои дела по сравнению с его делами яйца выеденного не стоят*».

Для передачи данных в ОГСПД рассматривали коммутацию каналов и коммутацию пакетов. При коммутации пакетов предпочтение отдавалось пакетам длиной 256 байт. В узлах коммутации предполагалась первичная обработка, в которой присутствовали арифметические и логические операции. Было известно, что все классические коды (Берлекэмпа, Рида, Соломона и др.) предназначены только для обнаружения и исправления ошибок при передаче и хранении информации, для арифметических операций было особое арифметическое кодирование, а для логических операций была известная гипотеза Элейеса (многократно затем доказанная), по которой для обнаружения k ошибок необходимо было к+1-кратное, а для исправления k ошибок 2к+1-кратное удлинение кода.

Предложенные нами коды Лагранжа, арифметические по построению, позволяют строить и максимальный вариант (это когда мощность множества ошибок совпадает с мощностью множества контрольных символов и между ними устанавливается изоморфизм). Интересен вариант с тремя контрольными символами, два из которых используются для исправления одиночной ошибки, а третий — для контроля правильности исправления одиночной или обнаружения кратной ошибки. Простейшая реализация алгоритма исправления одиночной ошибки получена при выборе 0-го и 1-го локаторов (по определению Амербаева В. М.) в качестве избыточных. Также удалось разработать алгоритм обнаружения и исправления ошибок при

логических операциях и появилась, таким образом, возможность говорить о сквозном повышении достоверности передачи данных в ОГСПД. А 256-байтный пакет для передачи получается при выборе в качестве модуля многочлена 8-й степени с двоичными коэффициентами.

Во время подготовки итоговых отчётов по программам ОГСПД и ОГАС Ю. Н. Черкасов вдруг сказал: «*Все коды, исправляющие ошибки, названы именами их авторов. Мы тоже должны так сделать*». И всюду название «*коды Лагранжа*» заменил на «*коды Амербаева — Бияшева*». Скромный Вильжан Мавлютинович просил этого не делать, но Юрий Николаевич умел проявлять упрямство. Так что во всех отчётах, одобренных и принятых государственной комиссией во главе с академиком Дородницыным А. А., это название так и осталось.

Но Вильжан во всех своих последующих работах использовал термин «*коды Лагранжа*»[1].

В дальнейшем вычислительные процедуры кодов Лагранжа применялись при разработке алгоритмов шифрования и формирования электронной цифровой подписи, которые были использованы для защиты информации в программном комплексе тестирования абитуриентов в Республике Казахстан.

Некоторые подробности этого есть в материалах конференции, посвящённой 50-летию СОК, которую проводил в качестве модератора Амербаев В. М. В отсутствие Акушского И. Я. и Юдицкого Д. И. Вильжан Мавлютинович остался безусловно СОК-овским лидером, глубоко и всесторонне понимавшим модулярные проблемы. Поэтому все, кого каким-либо образом интересовали дела СОК, обращались к нему по любому вопросу и всегда получали исчерпывающую информацию от этого удивительно широко эрудированного, доброго и внимательного человека. Таким он и останется в нашей памяти.

---

[1] А жаль. Приоритет и авторов, и страны оказался не защищён (прим. ред.).

Папа шёл по жизни с прямой спиной и улыбкой на лице

Бурмистрова (Амербаева) И. В.,
старшая дочь

Бурмистрова (Амербаева)
Ирина Вильжановна

В 1926 году тайно от родных поженились двое влюблённых. Девушке Ашраф было 16 лет, а юноше Мавлитдину — 18 лет. Они тайно убежали из Талды-Кургана в Алма-Ату. К сожалению, их первый ребёнок умер, а потом в 1931 году родился мой папа. Он был старшим братом в семье. После него родились Винера, Неля, Лейла, Варлен и Анвар.

Моя бабушка Ашраф, все звали её Рая, была женщиной исключительной доброты и терпения. Она родилась в семье богатого купца Ризы и его жены Марукай. У них в Талды-Кургане была большая усадьба. Мой папа рассказывал, что когда он там гостил в детстве, то запомнил много яблок и кур. Бабушка Марукай была очень доброй женщиной. У них в усадьбе регулярно останавливались красноармейцы на постой.

Ашраф Ризаевна до своего замужества получила хорошее образование. Когда они после свадьбы приехали в Алма-Ату, то оба начали учиться на рабфаках. Находясь у них в гостях, я видела в их доме газеты на арабском языке, которые выписывала Ашраф Ризаевна. Когда пошли детки, то Ашраф Ризаевна вынуждена была бросить учёбу, хотя училась отлично. А Мавлитдин Оспанович благополучно закончил обучение и защитил кандидатскую диссертацию. Он кандидат физико-математических наук. Все их дети получили высшее образование.

Мавлитдин Оспанович работал в Казахском государственном университете и в Казахском педагогическом институте. Много трудов и учебников по математике он перевёл на казахский язык. Надо сказать, что официальное имя дедушки было Мавлитдин. Но родные, друзья и коллеги по работе звали его Маулен. Поэтому у меня в памяти осталось это красивое имя.

Когда началась война, моему дедушке было 33 года и он ушёл на фронт. Он был артиллеристом. Мой папа очень любил своих родителей. Он тогда не умел молиться, но каждое утро он просил солнышко, чтобы его отец был жив. Дедушка прошёл всю войну и без единой царапины вернулся домой.

Бабушка Рая была очень доброй и никогда никого не ругала и не воспитывала. Папа рассказывал, что ему было неинтересно ходить в школу. Когда на экраны вышел фильм «*Свинарка и пастух*», папа вместо школы ходил в кино и каждый день смотрел этот фильм. Он влюбился в Ладынину. В результате его оставили в 5-м классе на второй год. Чтобы не расстраивать родителей, папа к сентябрю исправил в дневнике цифру V на VI. Его никто не контролировал. Но однажды в его отсутствие к маме пришли девочки из класса и открыли ей глаза. Папа этого не знал. Но как-то раз, когда он шёл очередной раз в кино вместо школы, он заметил свою маму, которая следила за ним. Ему стало очень стыдно. Когда он вернулся домой, мама ни слова ему не сказала. Но с тех пор папа стал регулярно ходить в школу. Когда начали проходить физику, папа влюбился в этот предмет. А для физики нужна математика. Перед ним открылся мир абстрактных чисел. Он увидел красоту и музыку формул. С тех пор математика стала его музой. В конце обучения он стал лучшим математиком школы.

С моей мамой они познакомились тоже благодаря математике. Мама в школьные годы болела и отстала от школьной программы. В 1947 году ей пришлось вернуться к этому вопросу. Она училась в педагогическом техникуме. Её товарищ посоветовал ей позаниматься дополнительно и порекомендовал Вильжана. Так они познакомились, а в 1953 году родилась я.

Я помню папу с самых ранних дней своей жизни. Мы с мамой жили в Алма-Ате, а папа учился в аспирантуре в Москве.

Однажды мама сказала мне, что скоро папа возвращается домой. Это было весной, перед майскими праздниками. Я помню радость и счастье, когда он приехал. Столько любви было в нём! Наша квартира как будто осветилась.

Когда я научилась читать, то, просыпаясь по утрам, первое, что я видела, были корешки книг. Я помню их названия: «Дифференциальные уравнения», «Ряды Фурье», «Операционное исчисление». Ничего не понимая, я знала, что это папины книги.

Когда мы ходили втроём в гости, папа начинал веселиться вместе со всеми, а потом потихоньку выходил из комнаты, находил себе уголок и начинал писать на листах бумаги что-то мне непонятное. Когда я подбегала к папе и начинала его отвлекать, он никогда не прогонял меня. Сажал на колени, обнимал, играл со мной. А когда я убегала, он снова начинал писать на листах бумаги что-то непонятное.

Мы жили втроём в однокомнатной квартире, которую нам дали мамины родители, временно уехавшие в Курган областной, т. к. дедушка уехал в длительную командировку. Дедушка работал в Заготзерне. Когда я родилась, дедушке было 43 года, а бабушке 41. Совсем ещё молодые.

Нам повезло. Молодой семье иметь отдельную квартиру всегда было роскошью. Друзья родителей часто приходили к нам не только в гости. Они приходили мыться (в те времена не у всех были душ и ванна), устраивали репетиции драматического кружка.

Самые счастливые воспоминания безмятежного детства — это я вместе с мамой и папой гуляем по парку им. М. Горького. Вокруг растут великолепные алма-атинские розы, тепло, я скачу на одной ножке, а рядом улыбаются мои родители.

В 1963 году родилась моя сестрёнка Оленька, и через год нам дали новую двухкомнатную квартиру рядом с академией наук. Я училась в 4-м классе и не понимала причин. Только потом я узнала, что папа защитил диссертацию и стал начальником лаборатории в академическом институте математики и механики.

В 1965 году состоялась встреча И. Я. Акушского, Д. И. Юдицкого и моего папы. Они обсуждали какую-то математическую

проблему. Гости из Москвы обозначили задачу. Папа рассказывал, что он всю ночь не спал. Ему была интересна проблема. К утру он нашёл решение и показал его Акушскому и Юдицкому. Они оценили молодого (34 года) математика и предложили работу в городе-спутнике под Москвой. Так мы всей семьёй в феврале 1966 года приехали в Зеленоград.

Зеленоград папа полюбил сразу и навсегда. Ему нравился лес. Он находил в лесу большие деревья — сосны, дубы. Разговаривал с ними. Несмотря на свою занятость, папа любил гулять в лесу. Один, с женой, детьми, внуками.

Интересы папы не ограничивались одними математическими проблемами. Его интересовали вопросы философии, психологии. С большим интересом папа изучал вопросы генетики, хотел вывести формулы генов...

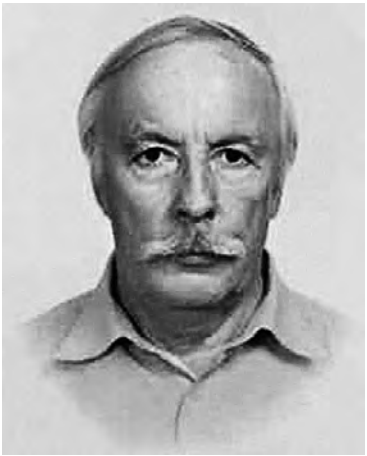
Папа с большим уважением относился ко всем религиям. Он обратился к Христу, потому что, по его словам, проникся состраданием к его судьбе. Он нашёл очень человечной жизнь Христа и выбрал православное христианство для своего дальнейшего духовного развития. В крещении он получил имя Владимир. Однако папа не относился к воцерковленным христианам. У него было своё собственное отношение к церковным обрядам.

На всех семейных торжествах папа всегда произносил тост за свою жену, которая родила ему дочерей, а те в свою очередь подарили ему внуков и правнуков. Папа очень любил их. Для каждого находил свой подход. Он всех нас любил. Делал подарки, радовался, когда мы заходили в гости, сразу звал пить чай.

Папа с уважением относился ко всем людям, независимо от их должности и социального статуса. Он всегда здоровался с уборщицами, в раздевалках с гардеробщицами, в магазинах с продавцами. Однажды на экзамене в МИЭТе он поставил слабенькой студентке «*хорошо*» только за то, что её звали Оля, как его дочь. Он всегда говорил, что он счастливый человек. Всю жизнь он занимался любимым делом. Папа шёл по жизни с прямой спиной и улыбкой на лице.

Соседство с Вильжаном создавало ауру солнечного света

Зверев Е. М.,
коллега по работе с 1972 г.



Зверев Евгений Михайлович

С Вильжаном я знаком со времён работы в СВЦ. Но непосредственное сотрудничество у нас началось где-то осенью 2002 года на предприятии ФГУП «НПЦ “СПУРТ”» (с 18.11.2002 г. по 17.01.2007 г.). Предприятие отпочковалось от НИИ микроприборов. В «СПУРТ» он занимал должность «главный научный сотрудник». Я руководил подразделением криптографической защиты информации. На тот момент работы выполнялись в интересах министерства обороны (несколько работ) и Центрального банка России.

Моя встреча с Вильжаном после долгого перерыва состоялась где-то в районе научного центра Зеленограда. Мы взаимно были рады встрече. Обменялись новостями о житье-бытье. Поговорили о прошлой технико-романтической жизни. Вспомнили нашего руководителя, а для меня и учителя — Давлета Исламовича Юдицкого. Вспомнили коллег и сотоварищей по работе над изделием 5Э53. Оценили плодотворность и энтузиазм работы того времени с точки зрения науки и техники. Побрюзжали на текущий момент и как бы на отсутствие особой научно-технической перспективы в работе текущего дня. Здесь я понял, что дела у Вильжана по работе, по зарплате весьма аховые и, самое главное, не просматривалась перспектива. А у меня был дефицит в думающих инициативных специалистах и особенно в математиках-криптографах. Он в то время погрузился именно в эти разделы математики. Я осторожно, боясь получить отказ,

предложил Вильжану работу в моем коллективе в «СПУРТ». К моей радости, Вильжан тут же с удовольствием согласился.

Буквально через день-два он вышел на работу. Сразу вписался в коллектив. Тут же разглядел научную заряженность сотрудников и актуальность выполняемых ими работ. В работу включился азартно, с большой энергией. Его интересовали все алгоритмические и математико-криптографические аспекты создаваемых средств защиты информации. Он замкнул на себя вопросы аналитических расчётов криптографической стойкости средств защиты. С математической точки зрения оценивал все крипто-алгоритмические новации технических решений вновь создаваемой шифртехники. Сам принимал участие и инициировал участие коллег в научно-технических мероприятиях — конференциях, симпозиумах, написании статей, агитировал и продвигал аспирантско-кандидатскую инициативу среди молодых разработчиков. Один из них Шарамок А. В., только что окончивший МИЭТ, уже готовивший диссертацию, тут же попал под научный «каток» Вильжана. Он срочно заставил его публиковать статьи, работать над совместными изобретениями, готовить доклады на конференции в Таганроге, МИЭТе и других организациях заказчика — МО и его НИИ. Под этот научный каток помимо Шарамка А. В. попали в недалёком прошлом его ученики по МИЭТу, а на тот день сотрудники и коллеги — Андрущенко Алексей, Ирина Любушкина (Грехнева). Все они также при участии Вильжана защитили диссертации (Андрущенко — магистерскую, Любушкина — кандидатскую).

Его научный «каток» действовал мощно и эффективно. Сам он с интересом увлёкся «*крипто-рюкзачными*» алгоритмическими конструкциями, актуальность которых уже была оспорена криптографическими аналитиками. Но он привнёс в эту теорию новые математико-алгоритмические элементы, тем самым продлевая их жизнеспособность. К этому делу он настойчиво привлёк и меня, хотя я не очень интересовался несимметричной криптографией. Написали с ним и с алмаатинцем Бияшевым Рустемом (нашим коллегой по совместной работе в СВЦ, также одержимым криптографией) несколько

совместных статей (см. библиографию Амербаева). Опубликованы они были как статьи в нескольких научно-технических изданиях не только России, но и в Республике Казахстан. С В. М. Амербаевым у нас вышел целый ряд статей и патентов. По многим именно он был инициатором и драйвером.

В 2005 году мы с Вильжаном и рядом других товарищей — разработчиков крипто-шифротехники переместились в фирму «АНКАД», где он работал на полставки. Полставки — это зарплата. А вот свой математический интеллект он отдавал на все сто процентов. То есть он также продолжал быть научно активным во всех отношениях, и особенно среди молодёжи. Вокруг него сразу образовалась когорта аспирантов, которым он инициировал научные диссертационно-кандидатские направления и которые органично вписывались в рабочую тематику предприятия. Двоих специалистов, прошлых своих аспирантов и успешно состоявшихся кандидатов технических наук, он увлёк, в дополнение к основной производственной деятельности, работой над докторской диссертацией.

Если работа была связана с новыми научно-техническими аспектами, он живо и инициативно включался в неё. У нас с ним в инициативном порядке появилась идея создать весьма эффективный по многим параметрам шифратор. Доказуемость его (шифратора) работоспособности должна была быть описана математически. Он в этом плане быстренько отодвинул меня в сторону, считая, что математика — это его конёк и конёк любимый, — стал решать задачу, невзирая на свою чрезмерную занятость. И задача была решена в считанные дни с положительным эффектом в пользу технической идеи.

В социально-человеческом плане В. М. Амербаева можно именовать Человеком с большой буквы. Он фактически, а не на словах был истинным христианином. Жил и поступал по заветам божьим, хотя церковную знать, как признавался мне, он не любил. Лично я за ним грехов никаких не видел ни в бытовой, ни в научной жизни. Мы с ним дружили. Обменивались мнениями на разные темы и даже по ряду сугубо личных тем.

Он очень любил свою семью, глубоко переживал любые её трудные или какие-то особые нюансы. Ну, например, зачихала

Зверев Е. М., Амербаев В. М. и Малашевич Б. М.
в музее ОАО «Ангстрем», 22.09.2011 г., Зеленоград

внучка, либо как-то проявило себя нездоровье супруги, либо ещё что-то. Он очень переживал. Это, пожалуй, единственное, что мешало его работе. Он искал способы им помочь.

А вот к своим болячкам он относился пренебрежительно и во многих случаях с юмором, с которым у него, кстати, всё было в порядке. Он как-то мне рассказывал, как он пошёл погулять по лесопарковой зоне. Это у нас, около работы фирмы «АНКАД». Вдруг он почувствовал себя совсем молодым и бодрым, а дух его именно таким и был. Этот собственный дух он решил проверить. Каким образом? А простым — он решил по тропе спуститься с одной горочки вниз оврага (овражьи горочки в этом лесу ну очень хороши и глубоки), но не по лестнице, которая там была для «*зрелых взрослых*», а напрямую — по склону. И вот тут случилась «*незадача*». Как он рассказывал: «*Одна нога что-то нашла на горке. Зацепилась. Ну, а далее все логично — покатился в полный рост вниз, под горку, чередуя голова-ноги-тело, голова-ноги-тело... и так далее. Подминая под собой сучки и палки лесной*

флоры». Первое, что он подумал и сказал про себя (а потом, некоторое время спустя, вслух и мне), когда поднялся, разогнулся и отряхнулся от земли: «*Больше я по лесу гулять не буду. Не хочу быть молодым...*». Правда, позже он рассказал мне о таком же «*пируэте*», который случился с ним ещё раз, но уже на лестнице в «АНКАД». Рассказ был примерно в том же духе, что и предыдущий, и также с юмором, при этом он сообщил, что вполне освоил дополнительную «*хлебную профессию*» каскадёра. Конечно, причиной этого чёрного юмора были его больные ноги.

Однако важно подчеркнуть — с Вильжаном никогда и ни в чем не бывало скучно. И это точно. Несмотря ни на какие жизненные перипетии, при любой погоде соседство с ним создавало ауру солнечного света и отсутствие каких-либо проблем. Это мои искренние ощущения — без преувеличений и натяжек.

О замечательном Учителе и Человеке

Инютин С. А.,
д. т. н., профессор,
ученик и коллега

Инютин Сергей Арнольдович

Непросто примириться с мыслью, что Вильжана Мавлютиновича нет с нами. Его сердце остановилось 14 декабря 2014 г. на 84-м году его насыщенной событиями и свершениями жизни.

Будущий академик Академии наук Казахской ССР и Национальной академии наук Республики Казахстан родился 25 апреля в 1931 году в г. Талды-Кургане Казахской ССР. Высшее образование получил в 1954 году по специальности «*математика*» в Казахском государственном университете на физико-математическом факультете, где в послевоенные

и последующие годы преподавали многие известные математики и механики, эвакуированные в Казахстан в годы войны. Университет, во многом благодаря этому кадровому потенциалу, давал фундаментальное механико-математическое и физико-математическое образование многим поколениям выпускников. Полученное качественное образование и тяга к новым знаниям позволили В. М. Амербаеву в 1959 г. поступить в аспирантуру МИАН СССР. В 1963 году он успешно защитил диссертацию по теме «*Численные методы обращения интегрального преобразования Лапласа*» и стал кандидатом физико-математических наук. В дальнейшем, вернувшись в Казахстан, он работал в Институте математики и механики республиканской академии наук заведующим лабораторией.

В 1971 г. в диссертационном совете НПО «Элас» Зеленоградского научного центра Министерства электронной промышленности СССР В. М. Амербаев защитил докторскую диссертацию на тему «*Вычисления в кольце главных идеалов и их приложения в вычислительной технике*». Вернувшись в Алма-Ату, он работал заместителем директора Института математики и механики Академии наук Казахской ССР.

Я имел честь познакомиться с Вильжаном Мавлютиновичем в 1976 году, когда поступил в аспирантуру математического института к члену-корреспонденту АН КазССР И. Я. Акушскому по научной тематике модулярной арифметики или системы остаточных классов. А в дальнейшем продолжил работу в научной лаборатории профессора, д. т. н. Ивана Тимофеевича Пака, друга и соратника Вильжана Мавлютиновича. Исследованиями в этой оригинальной научной области руководили члены-корреспонденты АН КазССР Амербаев Вильжан Мавлютинович и Акушский Израиль Яковлевич. Трудно переоценить их огромную роль по консолидации научных исследований и сплочению учёных и специалистов, выполняющих научные работы по модулярной тематике в различных городах большой страны: Москве, Киеве, Тбилиси, Минске, Львове, Зеленограде, Виннице и многих других. Мне повезло быть помощником, а иногда участником научных контактов и встреч, проводимых

Вильжаном Мавлютиновичем. Запомнился приезд в институт и беседа в отделении физико-математических наук Академии наук Казахстана с академиком В. М. Глушковым — директором киевского Института кибернетики АН УССР, всегда поддерживающим исследования по модулярной тематике в украинском кибернетическом центре. В институте для молодых научных сотрудников и аспирантов Вильжан Мавлютинович совместно с И. Т. Паком и А. Н. Казангаповым регулярно проводил расширенные научные семинары, на которых рассматривались новые идеи в области параллельных вычислений и вычислительных систем с нетрадиционной архитектурой. Анонсировалась и реферировалась достаточно редкая в те годы информация об отечественных и зарубежных проектах по перспективной и высокопроизводительной вычислительной технике. Запомнился детальный анализ под руководством Вильжана Мавлютиновича и Ивана Тимофеевича Пака идей Д. Кнута — автора восьмитомной библии компьютерной алгоритмики «*Искусство программирования для ЭВМ*». В широте научной тематики этих семинаров сказывалась глубина знаний самого Вильжана Мавлютиновича во многих областях современной компьютерной математики, которую обычно относят к области Computer science в западной терминологии. Монография Вильжана Мавлютиновича «*Теоретические основы машинной арифметики*», изданная в 1976 году в научном издательстве академии наук, для всех сразу задала очень высокую планку теоретического анализа проблем модулярной арифметики и показала перспективность применения методов современной алгебры к решению ряда научных проблем.

Вильжан Мавлютинович опубликовал шесть фундаментальных научных монографий и более 150 статей в нескольких научных областях: теория параллельных вычислений и архитектур, помехозащитное арифметическое кодирование, численные методы обращения интегрального преобразования Лапласа и решение сверхточных уравнений.

Необходимо отметить, что Вильжан Мавлютинович всегда с большим уважением и вниманием относился к казахским

национальным традициям, что вызывало ответное уважительное отношение коллег из академии наук республики. Мне довелось быть свидетелем, как в непростой период для всей страны и республики в конце 80-х годов прошлого века ученик академика Г. И. Марчука, директор ИММ АН КазССР академик У. М. Султангазин, избранный президентом республиканской академии наук, долго искал авторитетного математика с опытом руководящей работы. Проблема заключалась в том, что из-за болезни академика-секретаря О. А. Жаутыкова осталось без руководителя центральное физико-математическое отделение Академии наук Казахстана. На должность академика-секретаря ОФМН в 1987 году был приглашён В. М. Амербаев, одновременно он руководил отделом в Институте прикладной и теоретической математики АН КазССР. Выполняя функции его заместителя в научном отделе, я мог видеть, какое множество дел одновременно пришлось выполнять Вильжану Мавлютиновичу.

Все сотрудники его отдела старались помочь ему, но всё равно нагрузка была большой, трудные вопросы решал сам Вильжан Мавлютинович. Избранный в 1989 году академиком республиканской академии наук, он работал академиком-секретарём отделения физико-математических наук и членом президиума АН КазССР в непростой период с 1987 по 1993 годы. Необходимо особо подчеркнуть, что Вильжан Мавлютинович обладал очень широким научным кругозором. К его научным интересам относились: компьютерная математика и вычисления в алгебраических структурах, компьютерная алгоритмика обработки данных в модулярных кодовых форматах, помехозащитное кодирование со свойствами арифметической самокоррекции, информационная безопасность и криптография на базе модулярных пространств, вычислительные технологии в структурном проектировании микроэлектронных устройств.

В непростой обстановке после ликвидации Союзного государства Вильжан Мавлютинович первым осознал необходимость найти новые сферы приложения для модулярной арифметики. Эти приложения были обнаружены в области криптографии для вновь образованного министерства обороны

Казахстана. Инициатором работ по криптографии с модулярной спецификой стал В. М. Амербаев, под его руководством стало интенсивно развиваться взаимодействие с военными структурами республики, которым потребовался детальный анализ и модификации американских DES, ADES — алгоритмов защиты дискретной информации. Эта научная тематика успешно начала выполняться именно в его отделе.

На многие бытовые вопросы у Вильжана Мавлютиновича просто не хватало времени, поэтому очень медленно обустраивалась его новая квартира в экологически чистом районе Алма-Аты в предгорьях Заилийского Алатау. Рассказ был бы неполным, если бы не были сказаны теплые слова об Эмилии Нестеровне — супруге Вильжана Мавлютиновича. Созданный общими усилиями их дом с подлинно творческой научной атмосферой и душевной теплотой притягивал друзей и соратников, в него всегда было приятно прийти.

Вильжан Мавлютинович принципиально и требовательно относился к получению новых научных знаний, возражая кому-либо, он всегда уважительно аргументировал свои доводы и позицию. Довелось непосредственно почувствовать и мне это доброжелательное отношение к моим научным планам. В 2000 году после успешного выступления в подмосковной Черноголовке на научной конференции по параллельным вычислениям на секции академика В. В. Воеводина я поехал в Зеленоград к В. М. Амербаеву. Он благожелательно и конструктивно отнёсся к плану моей докторской диссертации и имеющимся наработкам, внеся ряд ценных замечаний. Это позволило развить предложения Вильжана Мавлютиновича о степенных модулярных системах по приложению идеи И. Я. Акушского о многоразрядных вычислениях с модулярными форматами в сверхбольших диапазонах изменения целых чисел. Был обоснован и разработан алгоритмический и программный инструментарий на модулярной основе.

Необходимо отметить, что, как у всякого долгоживущего перспективного научного направления, у модулярной арифметики были свои взлёты и периоды трудной, кропотливой работы. В 1991 году за цикл работ в составе группы учёных

Вильжан Мавлютинович был удостоен одной из последних Государственных премий — престижной награды СССР. После смерти И. Я. Акушского в 1992 году В. М. Амербаев взял на себя тяжёлую и ответственную задачу сплочения учёных-модулярщиков, работающих в России, а также в других независимых странах, бывших союзных республиках. Участвуя в 2003 году в работе международной конференции *Parallel Processing and Applied Mathematics* в городе Честехове (Польша), я убедился, что работы Вильжана Мавлютиновича хорошо известны в Польской академии наук, пересекаясь с некоторыми идеями академика Вацлава Серпинского, бывшего президента Польской академии наук.

Ведущая роль В. М. Амербаева в сплочении учёных, работающих по модулярной проблематике, была отмечена на Международной научно-технической конференции «*50 лет модулярной арифметике*», состоявшейся 23 ноября 2005 года благодаря непосредственному участию в ней Вильжана Мавлютиновича и его соратников из Научного центра микроэлектроники г. Зеленограда.

В. М. Амербаев с 1973 г. являлся профессором по кафедре прикладной математики. Под его руководством защищены 23 кандидатские диссертации, он был научным консультантом трёх докторских диссертаций. В последние годы Вильжан Мавлютинович работал профессором в НИУ МИЭТ, главным научным сотрудником в ряде научных организаций ИППМ РАН, НПИ «СПУРТ», где наряду с выполнением собственно научных исследований активно продолжал готовить молодую научную смену.

Научное сообщество, а особенно та его часть, которая долгие годы занималась исследованиями и приложениями модулярной арифметики, понесла невосполнимую утрату. Он был замечательным Человеком и Учителем с большой буквы, он сам учил молодёжь, и у него, активно работающего до конца жизни, многому учились. Наша общая задача — продолжить развитие дела, начатое трудами выдающихся учёных модулярного научного направления И. Я. Акушского, Д. И. Юдицкого и В. М. Амербаева.

Учёный, организатор, светлый и добрый Человек — в памяти навсегда

Искакова З. Д.,
учёный секретарь ОФМН НАН РК

Искакова Зоя Дюсембековна

В декабре 1988 г. меня, научного сотрудника Института ядерной физики (ИЯФ), вызвали в отделение физико-математических наук (ОФМН) Академии наук КазССР на приём к академику-секретарю отделения Вильжану Мавлютиновичу Амербаеву. Оказалось, что освобождалась вакансия учёного секретаря отделения и нужен был кандидат физико-математических наук, желательно кандидатура из физических институтов, так как другой учёный секретарь имел образование по специальности «механика». Вильжан Мавлютинович долго беседовал со мной и предложил мне эту должность. Для меня это было неожиданно, я колебалась: такая ответственность — работать в храме науки. Сверлила мысль: как я уйду из института, которым очень горжусь, и смогу ли я оправдать доверие, соглашаясь на предложение? Прошёл месяц, другой... Молчание, меня никто не вызывает, я успокоилась, продолжала работать в лаборатории академика Вениамина Моисеевича Кельмана, человека высочайшей культуры и интеллигентности.

Однако в отделение всё-таки была принята в апреле 1989 года. Оказалось, что на это место было несколько кандидатур. После долгих собеседований со всеми кандидатами, предварительно узнав мнения заведующего лабораторией академика Кельмана В. М. и академика Жетбаева А. К. (директора ИЯФ) обо мне, Вильжан Мавлютинович выбрал меня. Это он мне позже сказал.

Величие здания, ощущение, что ты ежедневно входишь в храм науки, окружение — академики, доктора наук, возглавлявшие

конкретные направления науки учёные, а также огромное количество документов и организационных вопросов — всё это внушало страх и постоянные мысли: справлюсь ли я с работой.

Вильжан Мавлютинович всегда входил в отделение с улыбкой, всегда был доброжелателен и корректен, никогда не повышал голоса.

С самого начала работы установились доверительные отношения, что настраивало на ещё более самоотверженную работу. Его хорошее отношение и поддержка помогли мне привыкнуть к новому месту работы.

Вильжан Мавлютинович учил анализировать, иметь собственное мнение, доверял самостоятельно решать некоторые вопросы и проблемы отделения. Он часто повторял, что учёный секретарь — это глаза и уши академика-секретаря, и приучил внимательно слушать всё на совещаниях и вникать в суть вопросов.

В 1989 году, когда я пришла в ОФМН, в состав отделения входили пять институтов: Институт математики и механики, Астрофизический институт им. В. Г. Фесенкова, Институт ядерной физики, Институт физики высоких энергий, Институт ионосферы.

Время было очень интересным и напряжённым, так как начиналась эпоха реформ в науке. Кроме координации научных исследований проводилось много организационных мероприятий.

В 1991 году в связи с огромным масштабом проводимых в Институте математики и механики научных исследований и наличием высококвалифицированных кадров по соответствующим научным направлениям из него были выделены Институт космических исследований, Институт проблем информатики и управления, Институт механики и машиноведения, Институт прикладной математики (г. Караганда), а сам институт переименован в Институт теоретической и прикладной математики.

Кроме того, в 1991 году был создан Физико-технический институт на базе физико-технического отдела Института физики высоких энергий и части научных подразделений по радиационному материаловедению Института ядерной физики. Передача подразделений во вновь созданный институт проходила очень

сложно, и только благодаря авторитету, человечности, доброжелательности и корректности Вильжана Мавлютиновича процесс был завершён на взаимных договорённостях.

Вильжан Мавлютинович очень много внимания уделял молодым кадрам. К нему часто приходили молодые специалисты за советами, делились планами. Особенно много внимания он уделял Малой академии, которая координировалась отделением физико-математических наук. Малая академия была организована для работы со школьниками: проводились семинары, олимпиады, конкурсы научных проектов.

Он организовл научный семинар «Проблемы динамического хаоса», способствовавший развитию направления «Проблемы эволюции открытых систем» (1996 г.), а также действующий до сих пор научный междисциплинарный семинар министерства образования и науки «Организация и эволюция природных структур» под руководством д. ф.-м. н. В. М. Сомсикова.

Вильжан Мавлютинович был очень скоромным и интеллигентным человеком. По случаю его юбилея в 1991 году никакого торжественного заседания в самой академии наук не было, торжественное заседание было проведено в Институте математики и механики, хотя многие, даже пятидесятилетие, старались провести его в зале заседания президиума. Я часто вспоминаю тот день. Когда после торжества мы шли на остановку (он часто отпускал водителя Анатолия Ивановича, ходил пешком), он с грустью сказал: «*Шестьдесят лет — кажется так много, а ведь душа совсем молодая*». Оказывается, это действительно так, но это понимаешь с годами.

Мы, сотрудники отделения, знали его любимых женщин — Эмилию Нестеровну и Винеру Мавлютиновну. Эмилия Нестеровна — статная, красивая, с синими глазами, вызывала у меня тихий восторг. Мне было очень приятно, когда я была приглашена к ним в гости в новую квартиру в микрорайоне «Самал».

В 1993 году, перед сменой руководства отделения, Вильжан Мавлютинович мне по секрету сказал, что скоро его сменит Станислав Николаевич Харин, что мне не нужно беспокоиться — с ним хорошо работать. Даже уходя, он проявил заботу, что не так часто бывает с руководителями.

В моей памяти Вильжан Мавлютинович останется не только как интеллигентный учёный, организатор, но и как светлый добрый Человек. Я благодарна судьбе, что жизнь свела меня с таким Человеком.

Вильжан, Вы горная вершина!

Коломыц В. Г.,
коллега по СВЦ и друг

Коломыц Виталий Георгиевич

Первая моя встреча с В. М. Амербаевым, точнее с его рабочим столом, на котором лежал огромный том великого математика Карла Фридриха Гаусса (1777–1855), произошла в 1966 г. в помещении, где первоначально размещался НИИ физических проблем (НИИФП). Хозяина стола рядом не было, но я сразу проникся огромным уважением к человеку, державшему на своём рабочем столе, как Библию, том Гаусса. Теория чисел, по-видимому, нужна была Вильжану для работы с «*остаточными классами*».

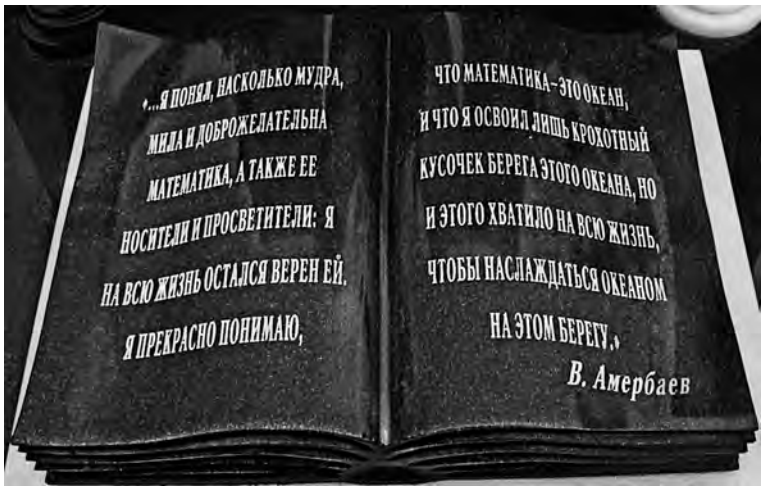
Вторая встреча была не у меня, а у моей сестры — абитуриентки МИЭТ. Она охарактеризовала Вильжана как внимательного и доброжелательного человека. На вступительных экзаменах по математике в МИЭТ он сделал абитуриентке маленькую подсказку (молча нарисовал линию), которая привела к успешному решению задачи. По-видимому, он рассуждал: пусть учится, время покажет, кто на что способен.

Третья встреча связана с нашим обращением к Вильжану с просьбой написать статью для книги «*Корни и крона Зеленограда*», посвящённой 50-летию города. Он согласился. Статья «*Зеленоград — город больших планов, надежд и дел на благо Родины*»

(опубликована и в настоящей книге) получилась очень содержательная, проникнутая любовью к Родине и к Зеленограду.

В дальнейшем моё общение с Вильжаном Амербаевым было более частым: на прогулках, на различных мероприятиях, в автобусе. За короткий отрезок времени езды от его дома до МИЭТа он так интересно рассказывал мне о математике, как никто другой.

Когда ветераны СВЦ узнали о кончине Вильжана, мы организовали серию обращений руководителей предприятий Зеленограда («Субмикрон», ИППМ РАН, «АНКАД», МИЭТ) и Академии наук Казахстана к префекту с просьбой похоронить его на особом «*нулевом*» участке основного городского кладбища среди заслуженнейших зеленоградцев. Просьба нашла понимание и была удовлетворена.



Фрагмент памятника[2]

Сейчас, часто бывая на кладбище, обязательно «*встречаюсь*» с Вильжаном у памятника на его могиле. Прекрасное монументальное произведение! Внизу в чёрной мраморной книге золотом высечены слова Вильжана, посвящённые математике и его преданности ей.

[2] Сокращённый из-за дефицита места вариант фразы, приведённой на стр. 4 книги.

В связи со скоропостижной и безвременной кончиной Вильжана я написал стихотворение, которое так и называется:

ВИЛЬЖАН

Это имя звучит, словно песня.
Мать над люлькой её сына-жана:
Расти, сынок, красивым, мудрым,
Называть тебя станут Вильжаном.
Мальчишка босиком по травам,
А пацаны кричат: Вильжан!
Соперники глядят ревниво.
Кто этот парень? Он Вильжан.
Он в среду родился на диво,
Когда и Бог не отдыхал,
Как плод трудов неповторимых.
Ему учёный статус дан.
Вот числа в вихре непокорном...
Кто укротит его? Вильжан.
По модулю сочтёт остатки,
В остатках — как в зерне пшеничном,
Найдёт закон, от всех отличный,
наш МАТЕМАТИК, наш Вильжан.
Седые шапки гор Тянь-Шаня,
В Алма-Ате садов наряд —
Везде Вильжан у себя, дома.
Он так любил Зеленоград!

17 декабря 2014 г., Зеленоград

А к выпуску настоящей книги у меня сложились следующие строки:

Вильжан, Вы горная вершина,
Недосягаема, но зрима —
И от подножья этих гор,
От зеленеющих лугов
И от цветков садов в долине.
Как романтический поэт,
Был в математику влюблён.

Ему даровано судьбой
Любить и сердцем, и душой,
Повсюду быть самим собой.
Его учёность сочеталась
С простой сердечной добротой,
С уменьем сложность объяснять
В доступной форме большинству,
Кто слушал и внимал ему.
Таким он был.
Вот так он жил...

9 января 2019 г., Зеленоград

Интересно и соответственно самому Вильжану значение его имени:

- Вильжан, Вильдан — дитя, ребёнок, служитель рая, юный (имя татарского происхождения);
- нумерология имени — ТВОРЧЕСКИЕ ЛЮДИ.

Таким творческим Человеком с большой буквы, служителем для людей с сердечной добротой, с вечно молодой душой он и останется в нашей памяти.

В. М. Амербаев и В. Г. Коломыц на 80-летии Д. И. Юдицкого

Человек необыкновенного таланта

Корнев М.Д.,
коллега по СВЦ

Корнев Михаил Дмитриевич

Вильжан Мавлютинович появился в СВЦ (специализированном вычислительном центре) г. Зеленограда в 1967 г., в тот период, когда коллектив центра получил заказ на разработку ЭВМ 5Э53 с баснословной по тем временам производительностью в 40 млн оп/с.

Такой производительности можно было достичь за счёт применения системы счисления в остаточных классах (СОК), которая была уже опробована в некотором урезанном виде и реализована в ЭВМ К-340.

Как известно, в СОК эффективно (за один такт работы арифметического устройства) реализуются так называемые модульные операции (сложение, вычитание, умножение), а немодульные операции (деление, сравнение чисел по величине, округление) занимают несколько тактов АУ и требуют достаточно сложных алгоритмов реализации.

Как раз на этапе разработки алгоритмов немодульных операций для 5Э53 у коллектива разработчиков, включая И.Я. Акушского, главного инициатора СОК, встретились значительные сложности: не получалось создать такие алгоритмы, которые одновременно были бы «быстрыми» по времени исполнения и требовали для реализации минимального оборудования.

Вот здесь как раз и проявился необыкновенный талант Вильжана Мавлютиновича, прекрасного математика с широким диапазоном знаний. Используя фундаментальные

достижения высшей алгебры и теории чисел, он достаточно быстро построил стройную теорию непозиционных систем счисления, включая работу в действительной и комплексной областях чисел, и определил направления для поиска эффективных алгоритмов.

Коллектив разработчиков под его руководством трудился очень слаженно, не считаясь со временем. Каждое его предложение сразу же просматривалось в аппаратуре, обсуждалось, находились плюсы и минусы. Вильжан Мавлютинович при этом вникал во все тонкости аппаратной реализации и снова отправлялся искать новые модификации алгоритмов.

В итоге поставленные задачи были эффективно решены и в дальнейшем реализованы в экспериментальном образце 5Э53. (Один из основных полученных алгоритмов получил прозвище «мастодонт»). Ряд разработчиков стали кандидатами, а Вильжан Мавлютинович защитил докторскую диссертацию.

С тех пор работы, связанные с непозиционными системами счисления (так называемой модулярной арифметикой), стали основными на протяжении всей его жизни.

Он был в курсе всех основных достижений в этой области и у нас, и за рубежом. Наряду с этим его интересовали многие направления развития информационных систем, микроэлектроники. В них он находил всё новые и новые применения модулярной арифметики и пытался, вникнув в конкретную специфику, решать актуальные задачи.

Главным направлением его деятельности становится разработка методов распараллеливания вычислений в целях достижения высоких показателей по быстродействию и надёжности в различных вычислительных средах, которые предоставляла микроэлектроника и информатика.

Круг его интересов обширен. Это не только область вычислительных средств специального назначения, но и такие области, как сжатие визуальной информации и поиск эффективных алгоритмов электронной подписи и шифрования данных в криптографии — областях, в которых очень сложно было получить новые результаты, так как человечество уже успело сделать здесь очень много.

Многих известных ему авторов, работавших в этих областях, он объединял своей энергией. В 2005 он году сумел организовать юбилейную международную научно-техническую конференцию «50 лет модулярной арифметике» с изданием трудов этой конференции.

Вильжан Мавлютинович был очень коммуникабельным человеком. Его не интересовали ранги людей, его интересовал сам человек. Работая с ним вместе на протяжении нескольких лет, я всегда видел его товарищеское заботливое отношение к людям, интерес к их работе, стремление помочь. Меня всегда восхищали его необыкновенная эрудиция, широкий кругозор и большой интерес ко всему новому.

Скрупулёзный учёный

Купчишин А. И., д.ф-м.н, профессор, академик МАН ВШ, директор ФТЦ КазНПУ им. Абая, член союзов писателей РК, РФ и евразийского союза писателей

С Вильжаном Мавлютиновичем Амербаевым я познакомился в восьмидесятые годы прошлого столетия. К этому времени он уже был доктором технических наук, профессором, довольно известным математиком и высококлассным специалистом по вычислительной математике, информатике и смежным вопросам. В частности, по следующим направлениям:

- Цифровая реализация интегральных образований и их обращений, включая сверхточные интегральные преобразования;

Купчишин Анатолий Иванович

- методы цифровой аподизации в задачах дистанционного зондирования, повышения разрешающей способности приборов, инвариантных к сдвигу;
- алгебраические методы повышения производительности вычислений в кольце целых чисел, гауссовых чисел и кватерионов;
- прикладные задачи алгебраического кодирования, включая помехоустойчивость;
- теоретические задачи криптологии; организация вычислений в квазигруппах, цифровые методы детерминированного хаоса в задачах криптографии и задачах математического моделирования генетических последовательностей.

Он был признанным учёным не только в Казахстане, но и во всём мире, пользовался заслуженным авторитетом и уважением в обществе. Мы нередко встречались с ним на различных совещаниях. Его всегда отличали скромность, простота, добродушие, приветливость и уважение к каждому человеку. Меня всегда поражала его восхитительная улыбка и жизнерадостный смех. Казалось, что он долгое время копит в себе свои чувства и в момент встречи выплёскивает их коллеге. В то же время в научных вопросах он был довольно принципиальным и щепетильным человеком и не терпел невежества и низкого уровня исследований. В таких ситуациях он преображался, а иногда даже и возмущался, но всегда при этом сохранял спокойствие и довольно в дипломатичной форме высказывал прямо в лицо своему собеседнику ошибки и замечания.

Помню, как-то вместе с академиком НАН РК Эрнстом Гербертовичем Боосом мы зашли к В. М. Амербаеву и попросили его выступить первым оппонентом по кандидатской диссертации «*Математическое моделирование некоторых задач физики космических лучей с использованием каскадно-вероятностного метода*» (по специальности — прикладная математика) нашего соискателя Анатолия Константиновича Ефимова, довольно известного программиста и преподавателя (Алма-Ата, КазНУ им. Аль-Фараби, 1993 г.). Не раздумывая ни минуты, он сразу же согласился, поскольку знал Анатолия лично. Много раз

Вильжан Мавлютинович вызывал к себе А. К. Ефимова для бесед, задавал большое количество вопросов, а после сам тщательно выводил и анализировал практически все наши формулы. Как правило, все они были связаны с теорией вероятностей. Мы этому с Э. Г. Боосом были очень сильно удивлены. В связи с защитой Анатолия Константиновича вспоминается такой случай. Буквально за несколько недель до защиты на имя председателя совета академика НАН РК, профессора Алексея Тимофеевича Лукьянова поступила жалоба от одного из известных физиков о том, что в диссертации А. К. Ефимова представлены старые, уже давно защищённые другими учёными результаты. Был организован семинар, на который пришли и мы с Эрнстом Гербертовичем. В. М. Амербаев и один из членов совета, академик из Киргизии (детально изучившие диссертационную работу), были сильно возмущены поведением жалобщика и готовы были дать ему серьёзный отпор. Узнав о готовящихся выступлениях, тот на семинар не явился. В итоге всё закончилось благополучно.

В 1990 году я и Э. Г. Боос обратились с просьбой к В. М. Амербаеву быть оппонентом по диссертации Татьяны Александры Шмыгалевой по теме «*Исследование и особенности расчёта на ЭВМ каскадно-вероятностных функций с учётом потерь энергии*», представленной на соискание учёной степени кандидата физико-математических наук по специальности 05.13.16 «*Применение вычислительной техники, математического моделирования и математических методов в научных исследованиях*». Защита проходила в специализированном совете КазГУ им. С. М. Кирова (ныне это КазНУ им. Аль-Фараби) под председательством академика НАН РК, профессора А. Т. Лукьянова. Диссертация Вильжану Амербаеву очень понравилась. Он проштудировал её, как говорится, от корки до корки, в том числе все выводы формул и сами формулы, алгоритмы и программы. Его поражало то, что все полученные теоретические расчёты удовлетворительно описывали большое количество экспериментальных данных. Это вызывало у него не только огромное удивление, но и большой восторг. При дальнейших встречах он неоднократно спрашивал меня: «*Анатолий! Я вижу, что в ваших*

формулах и расчётах нет ни одного свободного параметра, есть лишь только определённые приближения и допущения. Как так получается, что такие громоздкие формулы могут довольно успешно описывать экспериментальные кривые?» Одно время он даже хотел серьёзно поработать в нашей команде и применить свои знания и опыт в развитии и создании каскадно-вероятностного метода. Жаль, планы поменялись, и он уехал работать в Зеленоград в Московский институт электронной техники.

Но связи наши не прерывались. Мы продолжали общаться, правда, значительно реже. В 2001 году Вильжан Мавлютинович выступил первым оппонентом у нашей соискательницы Т. А. Шмыгалёвой по диссертации «*Математическое моделирование радиационно-физических процессов в различных средах*», представленной на соискание учёной степени доктора технических наук по специальности 05.13.18 «*Математическое моделирование, численные методы и комплексы программ*». Защита проходила в диссертационном совете Института математики МОН РК под председательством заместителя директора этого института доктора физико-математических наук, профессора Ивана Тимофеевича Пака. В. М. Амербаев дал высокую оценку работе Т. А. Шмыгалёвой. Правда, перед приёмом к защите один из математиков пытался доказать, что диссертация слабая и не удовлетворяет требованиям ВАК РК, но это у него не получилось, в значительной степени благодаря принципиальности, помощи и усилиям Вильжана Мавлютиновича.

Приведу ещё один случай. В конце восьмидесятых годов на одну из научных тем, руководимой Э. Г. Боосом, поступил отрицательный отзыв с рядом общих замечаний (как потом выяснилось, замечания были написаны по определённым личным мотивам, не имеющим никакого отношения к науке) от рецензента и довольно близкого ему человека. Эрнст Гербертович был сильно расстроен и позвонил мне. Голос его дрожал. Он с недоумением рассказывал мне: «*Я никогда не ожидал такой подлости от этого человека, можно даже сказать друга. Как же он мог такое написать? Ведь это все неправда*». Я его успокаивал как мог. В конце концов мы решили пойти к академику-секретарю физико-математического отделения Национальной академии

наук В. М. Амербаеву (тогда он занимал эту должность) и посоветоваться с ним, что делать дальше. Он уже был в курсе дела и, очень внимательно нас выслушав, показал отзыв на годовой научный отчёт (как потом оказалось, это был тот же самый человек, что и в случае с А. К. Ефимовым). Под угрозой увольнения оказалось около десяти сотрудников лаборатории физико-технического института НАН РК, которой заведовал Э. Г. Боос. Его можно было понять. Естественно, мы разнесли в пух и прах все замечания оппонента, детально аргументируя наши ответы. Вильжану Мавлютиновичу нетрудно было во всём разобраться, и он согласился с нашими доводами, дав положительную оценку годовому отчёту (с учётом рецензий других специалистов).

В те далёкие годы я неоднократно беседовал с В. М. Амербаевым не только на научные, но и чисто человеческие темы. Он нравился всем людям — и крупным учёным, и рядовым сотрудникам, специалистам и простым работникам. Любил рассказывать об успехах молодых исследователей, интересовался их делами, бытом, семьёй. Как-то мы заговорили о трудностях общения с друзьями и коллегами, живущими в других городах и странах. В то время ещё не было электронной почты, Интернета. Можно было только звонить, давать телеграммы и писать письма, что мы неоднократно и делали.

Я посвятил ему стихотворение (песню):

ПИСЬМА
Вильжану Амербаеву

Старое слово какое — письмо,
Стало уже забываться оно.
Только вот строчка, как детство, свежа,
Всё пролетело в мгновенье, а жаль.
Помню отчётливо каждое сам —
Много когда-то я их написал.
Шло всё от сердца, писалось не зря
Маме и папе, подругам, друзьям.
Сколь перевидел их наш белый свет,
Что тут такого? — Обычный конверт.

Чуть надорвал его — вынул нутро,
Листик бумаги, в нём несколько строк.
В них и рассвет, и вечерний закат,
Слезы и радость, печаль и тоска.
Нежность, забота, добро или зло.
Все, что бывает, что было, прошло.
Письма — души нашей выжженной часть,
Их почему-то не пишут сейчас.
Шлют телеграммы, но мне не понять,
Лишь телефонные трубки звонят.
Письма храню, будто старый аскет,
В добром забытом своём сундуке.
И недоволен порою собой.
В них — моя жизнь, моя радость и боль.

6.05.95
(Из книги «*Вспоминай обо мне*», Алма-Ата, 1995)

В свободные минуты, размышляя о нашем бытии, быстротечности времени, я часто вспоминаю Вильжана Мавлютиновича, его доброту, улыбку, располагающую к общению, к беседе. И в будни, и в праздники он мчался в небыль, в диво, создавая каждый день что-то новое, отдавая всего себя без остатка работе, даря людям, семье и друзьям радость и надежду.

Ему не страшны были грозы, опасности и повороты.

ПАДАЕТ ВРЕМЯ
Вильжану Амербаеву

Реет задорное племя,
Грезит восторгами небо.
Падает время
В небыль.
Рвётся порыв на арену,
Мечется пыл нерадивый.
Падает время
В диво.

Месяц засыпала древность,
Тучи завесили нудность.
Падает время
В будни.
Стонет и вертится стремя,
Жалят дожди и морозы.
Падает время
В грозы.
Плачет усталое бремя,
Год не один в стрессах прожит.
Падает время
В пропасть.
Мечется разум мой бренный,
Вдаль устремляя обеты.
Падает время
В бездну.

6.03.14

(Из книги «*Мчится ветер по рассвету*», Алматы, 2014)

К восьмидесятилетию я, Т. А. Шмыгалёва и А. И. Акишев написали от имени друзей и коллег поздравительный адрес В. М. Амербаеву и отправили его в Москву. Позже, во время нашего телефонного разговора, он подтвердил получение адреса. Привожу его текст (в подлинном варианте):

«Уважаемый Вильжан Мавлютинович!

Сборная команда Казахстана по науке и образованию (из числа Ваших близких друзей, знакомых и коллег) шлёт Вам горячий привет с Вашей Родины — Республики Казахстан, и от всей души поздравляет Вас с юбилеем — 80-летием со дня рождения и 55-летием научно-организационной, педагогической и общественной деятельности.

Вся Ваша жизнь — это образец беззаветного служения науке и образованию. Окончив физико-математический факультет Казахского государственного университета им. С. М. Кирова и аспирантуру Математического института им. В. А. Стеклова, Вы навеки связали свою жизнь с вычислительной математикой, компьютерной алгеброй, цифровыми методами обработки сигналов

и информатикой, достигли огромных успехов и получили мировое признание.

Защитив кандидатскую, докторскую диссертации и став сначала членом-корреспондентом, академиком АН КазССР и академиком-секретарём АН КазССР, Вы внесли огромный вклад в дело развития науки и подготовки научно-педагогических кадров в Казахстане.

Ваши монографии «Основы машинной арифметики комплексных чисел», «Операционное исчисление и обобщённые ряды Лагерра», «Теоретические основы машинной арифметики», «Распределение регулярных потоков сообщений в информационных системах», «Численный анализ лагерровского спектра», «Параллельные вычисления в комплексной плоскости» и др. стали классическими пособиями для молодых учёных — математиков-информатиков, начинающих серьёзно заниматься научными исследованиями.

Вы создали серьёзную научную школу и выпустили огромную армию кандидатов и докторов наук.

Главные Ваши качества — высокий профессионализм, скрупулёзность, педантичность, высокая человечность и порядочность, доброта, простота и любовь к людям, снискали к Вам огромное уважение среди Ваших коллег-учёных, друзей и учеников.

Дорогой Вильжан Мавлютинович!

В день Вашего юбилея желаем Вам крепкого здоровья, долгих лет жизни, дальнейших творческих успехов, счастья и благополучия.

Знайте, что на Вашей Родине — в Казахстане помнят и любят Вас и всегда будут помнить и любить Вас. Вы вечно будете жить в наших сердцах и душах.

Ваши друзья и коллеги:
академик МАН ВШ, д.ф.-м.н., проф. Купчишин А. И.,
академик МАИ, д. т. н., проф. Шмыгалёва Т. А.,
д. ф.-м. н., проф. Акишев А. И.»

К великому сожалению, жизнь человека не вечна и когда-то кончается. Все мы уйдём из этого мира в иной мир, откуда не возвращаются. В. М. Амербаев оставил глубокий след на нашей планете. Пусть земля ему будет пухом. Светлая память о нём навсегда сохранится в наших сердцах.

Всегда активен и жизнерадостен

Куцепалов Н. О.,
коллега по работе в фирме «АНКАД»

Куцепалов Никита Олегович

Заочное знакомство с Вильжаном Мавлютиновичем Амербаевым началось в МИЭТе, в главном корпусе которого расположена доска почёта самых заслуженных преподавателей нашего института. Среды прочих, разумеется, был и Вильжан Мавлютинович, его фотография была запоминающейся из-за его искренней улыбки и восточной внешности.

Позднее в 2009 году во время прохождения преддипломной практики я начал работать в Фирме «АНКАД», где трудился и Вильжан Мавлютинович. Долгое время рабочего контакта с Вильжаном Мавлютиновичем у меня не было, но было явно заметно, что, несмотря на возраст, Вильжан Мавлютинович активно взаимодействует с различными сотрудниками фирмы и института. В моё время с ним вели активную работу Шарамок А.В и Тюфякин Д. Н., а также не раз я видел, как студенты и аспиранты МИЭТ приходили к нему на консультацию.

В 2013 году одним осенним днём я подвозил Вильжана Мавлютиновича домой. Он спросил, интересно было бы мне заняться научной деятельностью. В этом весь академик Вильжан Мавлютинович, до последнего дня, с интересом и энергией занимающийся сам и привлекающий всех заинтересованных, преданный Науке. В тот момент я взял паузу, чтобы возобновить с ним взаимодействие летом 2014 года.

Летом 2014 года мы начали взаимодействие, научное направление было выбрано Вильжаном Мавлютиновичем — *применение кватернионных вычислений в целях построения крипто-алгоритмов.* С первых дней работы с Вильжаном Мавлютиновичем я обратил внимание на многогранность его деятельности — это и научные статьи для фирмы «АНКАД», НИУ «МИЭТ» и ИППМ РАН, и участие в НИРах, проводимых Казахской НАН, и инициативные научные работы.

И в последний рабочий день Вильжана Мавлютиновича, это была пятница, мы обсуждали проблемы данного направления, Вильжан Мавлютинович был, как всегда, активен, жизнерадостен, и даже мысли не было, что жизнь этого человека закончится менее чем через два дня.

В заключение хотел рассказать об одном случае: поздней осенью 2014 года Вильжан Мавлютинович попросил проводить его до остановки. По пути он рассказал, что у него есть проблемы со зрением — в сумерках он практически ничего не видит. От фирмы до автобусной остановки недалеко, но мы останавливались около десятка раз — дорога давалась ему нелегко, у Вильжана Мавлютиновича были проблемы с сердцем. Но всё это не мешало Вильжану Мавлютиновичу оставаться активным сотрудником многих предприятий города Зеленограда и Казахстана. Дай бог всем иметь такие цели и мужество в их достижении!

Мне посчастливилось учиться у него

Любушкина И. Е.,
к. т. н., гл. специалист фирмы «АНКАД»

Каким он был человеком

Любушкина Ирина Евгеньевна

Думая о Вильжане Мавлютиновиче, я вспоминаю его добрую улыбку и душевную теплоту, которой веяло от него. Рядом с ним казалось, что мир наполнен добротой, терпением и что нет таких задач, с которыми невозможно справиться. Общение с ним вселяло в меня уверенность в своих силах, способностях, дарило вдохновение и заставляло идти вперёд к новым целям.

Несмотря на возраст, Вильжан Мавлютинович был полон оптимизма, желания развиваться и идти вперёд. И этими качествами он щедро делился с окружающими, особенно со своими студентами и аспирантами. Для всех, кто обращался к нему, он находил время, силы, предлагал интересные задачи, помогал взглянуть на проблемы под другим углом зрения. Огромный опыт и невероятное понимание других людей позволяли ему находить для каждого интересное направление для исследований.

Мой опыт общения с В. М. Амербаевым

Мне посчастливилось учиться у него на протяжении многих лет. Моё знакомство с ним началось во времена моей учёбы в Московском институте электронной техники (МИЭТ). Вильжан Мавлютинович читал кур лекций по прикладной криптографии в рамках специальности «*организация защиты*

информации». Целью курса было знакомство студентов с азами криптографии, криптологии и криптоанализа. Он легко и интересно преподносил нам основные математические понятия и теоремы, на которых базируется криптография. Эти лекции стали для меня пропуском в обширный мир информационной безопасности. Знания, полученные на данном курсе, до сих пор помогают мне разбираться в современных математических направлениях шифрования и защиты данных.

Дальнейшее моё общение с Вильжаном Мавлютиновичем продолжилось во время моего обучения в аспирантуре. Вильжан Мавлютинович был моим научным руководителем и помогал работать над диссертационной работой. Моя диссертация была посвящена исследованию и разработке методов, направленных на повышение уровня защищённости каналов сигнализации системы спутниковой связи, разработанной без учётов современных требований по защите информации. При этом данные методы должны были учитывать ограничения, накладываемые системой спутниковой связи, и обеспечивать минимальное влияние на функционирующие протоколы и алгоритмы связи.

Вильжан Мавлютинович принял активное непосредственное участие в написании двух разделов моей диссертационной работы:

1) метод защиты от корреляционного прослушивания каналов сигнализации;
2) интерполяционная защита от воздействия имитационных помех многоканального ствола.

Фактически он стал идеологом заложенных в данных разделах математических идей. Моим вкладом в проделанную работу была адаптация разрабатываемого им математического аппарата под систему спутниковой связи, для которой строились методы защиты, и проведение вычислительных экспериментов синтезированных алгоритмов.

Последние наработки

В последние годы Вильжан Мавлютинович прорабатывал идеи многомерного шифрования и гомоморфных модуль-

ных преобразований, которые можно было бы применять в криптографии.

Многомерное шифрование в его интерпретации расширяло понятие сетей Фейстеля. Предлагалось строить двумерную или трёхмерную матрицу узлов. Каждый узел характеризовался набором параметров: ключ преобразования Ki и функция преобразования f(Ki, xi). При этом данные параметры могли быть открыты и известны противнику. Секретной частью многомерного шифрования являлась траектория прохождения по матричным узлам. В каждом узле входные данные преобразовывались с помощью присвоенных конкретному узлу параметров, на выходе получалась многократно преобразованная информация. Расшифрование подразумевало прохождение узлов в обратном порядке. Для разных пользователей определялись свои траектории, которые обеспечивали уникальность шифрования.

В качестве гомоморфных модульных преобразований Вильжан Мавлютинович предлагал использовать математический аппарат кватернионов. Данная математика в последнее время начала широко применяться для обработки многомерных сигналов. Идея состояла в том, чтобы расширить модульные вычисления, применяемые в криптографии, построить ряд алгоритмов и провести вычислительные эксперименты.

Данная задача объединила вокруг Вильжана Мавлютиновича группу заинтересованных студентов и молодых инженеров. Были достигнуты определенные наработки, которые демонстрировались вычислительным экспериментом. К сожалению, Вильжану Мавлютиновичу не суждено было продолжить работу над этой темой. Но тот глубокий научный задел, который он оставил после себя, до сих пор помогает нам совершенствовать вычислительный базис, применяемый в системах защиты информации

Ещё об одной стороне большого Учёного

Макаренко Н. Г.,
д. т. н.

Макаренко Николай Григорьевич

В 1994 году в Институте теоретической и прикладной математики (ИТПМ, г. Алма-Ата, КазССР) начала работать междисциплинарная программа «*Динамический хаос в распределённых системах*». Инициатором и руководителем программы был Вильжан Мавлютинович. Лично для меня он был не просто руководителем программы и не только человеком, который убедил меня перейти в ИТПМ, но и моим Учителем. Я расскажу о своём участии в этой программе, которая существенно изменила мою научную карьеру.

После окончания Уральского государственного университета (г. Свердловск) у меня было несколько руководителей. Первым был Григорий Моисеевич Идлис, директор Астрофизического института им. В. Г. Фесенкова (АФИФ, г. Алма-Ата), куда я попал по распределению. Это был учёный с широким кругозором. Он возглавлял отдел динамики звёздных систем, но занимался ещё наукометрикой, антропным принципом и многими другими интересными вещами. Директор — всегда человек занятый, тем более что обстановка в институте в те годы была весьма непростой. Предполагалось, что я займусь моделями приливного взаимодействия нашей Галактики с её ближайшими спутниками — Магеллановыми Облаками. Предложенные Григорием Моисеевичем задачи не вызвали у меня особого интереса, и я увлёкся главным образом самообразованием. При этом я и мой руководитель старались не докучать друг другу. И это у нас хорошо получалось! Я с увлечением

изучал те разделы математики, которые казались мне интересными и которые обычно не входили в обязательные курсы для физиков. Я не знал, да и до сих пор не могу объяснить, почему я это делал. Теперь, мне иногда кажется, что кто-то вёл меня за руку по запутанным тропинкам сада абстрактной математики. Ненужных вещей не бывает, как заметил в своё время Марк Аврелий, римский император и философ. Просто следует из всех ненужностей уметь отобрать самое необходимое, когда возникнет подходящая ситуация.

Для меня такая ситуация возникла в конце 1980-х годов, когда я ещё работал в АФИФ. В это время в моду начали входить детерминированный хаос и мультифракталы. Я не оговорился, мода всегда была и есть в науке! После отъезда Г. М. Идлиса в Москву в Институт истории естествознания и техники АН СССР его преемником на посту директора и моим новым руководителем стал Тукен Бигалиевич Омаров. Он был специалистом по небесной механике и занимался популярной в то время задачей о движении двух тел с переменной массой. Замечу, что в те времена получение нового интегрируемого, в квадратурах, случая в небесной механике было значительным достижением, достаточным для получения степени кандидата наук. Мне опять не повезло, потому что и в этой области я не смог найти для себя интересной задачи. Я думаю теперь, что причина была в возрастной лени: с защитой кандидатской *в срок* у меня не получилось, а писать «*кирпич*» на диссертабельную, но не интересную для меня тему, я просто не хотел.

И вот я узнаю, что в ИТПМ начал работу семинар, посвящённый «*модным*» направлениям, связанным с нелинейностью, фракталами и самоорганизацией критичности. Руководителем семинара был Вильжан Мавлютинович. Уже после первых посещений заседаний семинара я с удивлением обнаружил, что вещи, с которыми я познакомился в последние годы, лежат в основе понимания новых концепций, которые обсуждались на семинаре.

Здесь уместно немного подробнее остановиться на этих вещах. Они были связаны прежде всего с подходами к моделированию динамических систем. Традиционные линейные модели отягощены догмами классической аналитики. Основная из них

утверждала, что *всё, что происходит, может быть и сказано*, т. е. выражено на языке математических символов. Нетрудно усмотреть в том метафору известного тезиса Тьюринга — Чёрча. Известная «*непостижимая эффективность математики в естественных науках*», отмеченная Юджином Вигнером, была обязана как раз моделям, заданным дифференциальными уравнениями. Особую важность приобретает здесь теорема о существовании и единственности решения. Она гарантирует вам, что если делать всё правильно, полученное решение будет единственным и обладает нужными вам свойствами. Цена такого подхода оказывалась в большинстве интересных случаев весьма значительной. Так, приходилось упрощать исходные уравнения, пренебрегая малыми членами, либо исключать «*несущественные*» связи. Итогом таких процедур, как правило, было так называемое линейное приближение, весьма далёкое от той ситуации, которую мы собирались описать.

Немногочисленные известные нелинейные случаи были связаны с системами, имеющими много степеней свободы. Они описывались обычно уравнениями гиперболического типа и редуцировались к приятным случаям в рамках линейного приближения. Ситуация коренным образом изменилась в конце 1970-х годов, когда с помощью компьютерных экспериментов были сделаны два значительных открытия, которые породили две новые теоретические конструкции: *солитон* и *странный аттрактор*. Оказалось, что даже в системах детерминированных уравнений с небольшим числом степеней свободы может возникать стохастическое поведение. Если их решения сильно зависят от начальных условий, то малые погрешности начальных данных экспоненциально растут в фазовом потоке так, что начиная с некоторого момента времени будущее состояние системы становится непредсказуемым. Траектории такой системы заполняет низкоразмерное притягивающее множество в фазовом пространстве — *аттрактор*. Траектории на аттракторе разбегаются в одних неустойчивых направлениях и сжимаются в других, устойчивых. Вследствие диссипации сжатие преобладает и в устойчивых направлениях аттрактор копирует сам себя. Сечение фазового потока приобретает самоподобную (*странную*)

структуру канторова множества с дробной размерностью. Эти идеи легли в основу концепции *динамического хаоса*.

Большой интерес к странным аттракторам был вызван по меньшей мере двумя обстоятельствами. Во-первых, большинство типичных природных систем являются диссипативными и описываются нелинейными уравнениями. Таких уравнений много, но сценарии перехода к хаосу определяются типами нелинейности, которых относительно мало. Следовательно, асимптотические режимы таких систем в определённом смысле можно классифицировать. Во-вторых, и это очень важно для приложений, появился метод восстановления образа аттрактора по проекции фазовой траектории на произвольное направление, т. е. по временному ряду. Формально такая реконструкция представляет собой дифференцируемое вложение ряда в обычное евклидово пространство соответствующей размерности. Метод реконструкции аттрактора из скалярных временных рядов как эвристический сначала был предложен в 1980 г. группой Паккарда. Год спустя он стал строгим, а именно после статьи Флориса Такенса, который обобщил на динамические потоки и каскады знаменитую теорему Уитни о вложении дифференцируемых многообразий.

Новый способ построения модели из наблюдаемого сигнала быстро инициировал совершенно новую область численных методов топологической динамики — *эмбедологию*, от английского слова *embedding* (вложение). Техническая сторона эмбедологии основана на богатом арсенале разработанных ad hoc алгоритмов для численных методов оценки динамических инвариантов аттрактора. На базе алгоритма Такенса возникли новые нелинейные методы анализа временных рядов и нелинейная многомерная техника прогноза временных рядов. Таким образом, экспериментатор смог получить универсальную модель системы прямо из наблюдения, почти в точности следуя узникам *пещеры Платона*. Как известно, им были доступны лишь тени внешнего мира, которые они видят на стене. Тени были единственными источниками сведений об окружающем мире. Проблема заключалась в том, чтобы установить, что в действительности происходит снаружи.

С другой стороны, структура странных аттракторов была связана с идеями фрактальной геометрии. Первые работы в этой области были опубликованы французским и американским математиком Бенуа Мандельбротом в 1975 г. Он обратил внимание, что природные объекты вовсе не являются образами гладкой геометрии: «*Облака не сферы, горы не конусы, береговые линии не окружности, древесная кора не гладкая, и молния далеко не прямая... Природа демонстрирует нам не просто более высокий, а совершенно иной уровень сложности*». Созданная им фрактальная геометрия пришлась как раз «*ко двору*» хаотической динамики.

И вот все эти интересные новинки стали предметом дискуссий на семинарах. Они открывали новые пути к построению моделей динамических систем — из первых принципов, т. е. прямо из наблюдений. Новые знания можно получать прямо из таблиц данных! В истории науки это удалось впервые немецкому математику Иоганну Кеплеру, который вывел три своих знаменитых закона из наблюдений Тихо Браге. Разумеется, для этого нужен был некоторый эвристический контекст, а следовательно, и символы веры. Эмбедология также опирается на символы веры, которые именуют кредо идеального экспериментатора. Оно основано на математических понятиях и правдоподобных предположениях, не сводящихся к аксиомам. Сама идея о символах веры, как пролегомен строгого формализма, выглядит несколько необычно. Впрочем, необычной является и концепция фрактала как предельного образа или аттрактора системы итерирующихся отображений Барнсли — Хатчинсона.

Вильжан Мавлютинович формировал в нас новое мировоззрение настолько деликатно, что переход к новым идеям прошёл почти безболезненно. Большая часть исследователей всегда ориентирована на ожидания: нам хочется увидеть в любой новой идее существенный прорыв, новые горизонты. Вильжан Мавлютинович учил нас, что для практических задач более важны предубеждения. Точнее, ограничения области, за пределами которой новые подходы могут дать ложные результаты. Сперва это казалось нам необычным. Позднее мы поняли мудрость нашего наставника: здоровый скепсис приносит в итоге больше пользы, чем неоправданные ожидания.

Мне запомнилась одна наша беседа с моим Учителем. Я не помню подробностей, но речь шла о двух точках зрения на полезность математики. Первая указывала на преимущества решения конкретных задач — они помогают лучше понять аналитику. Вторая сводилась к утверждению, что первичной является как раз аналитика. Именно она помогает в решении конкретных задач. Позднее я нашёл похожее обсуждение у замечательного математика У. Т. Гауэрса в его замечательном эссе «*Две культуры в математике*». Я посетовал, что мне не очень нравится доказывать теоремы. Потому что послевкусье многих доказательств содержит элементы магии, о которой писал Анри Пуанкаре. А именно: полученное доказательство выглядит вполне приемлемым с точки зрения аналитики, но вот неясно, почему именно посылками явились, скажем, A, B и C и использовались они именно в выбранном сочетании? Вильжан Мавлютинович выслушал меня и сказал, что мне лучше вообще не заниматься выводом теорем. Решение конкретных задач получается у меня гораздо лучше. Я успокоился, и вот до сих пор следую этому мудрому совету. И, как мне кажется, довольно успешно.

Год спустя после начала семинаров Вильжан Мавлютинович предложил мне перейти в ИТПМ в его лабораторию. Я с удовольствием принял его предложение и полностью переключился на проблемы, которые оказались мне удивительно близки.

В те годы сам Вильжан Мавлютинович увлёкся «*вечной*» проблемой универсальности генетического кода. Одной из интригующих загадок в этой задаче является так называемая вырожденность кодонов: биологи находят всего 20 аминокислот из 64 возможностей кодирования триплетами из 4 типов нуклеотидов. Вильжан Мавлютинович предложил оригинальную спецификацию, опираясь на вложимость вырожденности в структуру некоторой мультипликативной группы.

Исключительная интуиция в выборе интересных тем и продуманная тактика управления программой позволили объединить в ней совершенно разных по характеру и по интересам молодых и не очень молодых учёных из различных институтов Алма-Аты. Участники программы занимались обобщениями классических сценариев хаоса (Панкратова И. Н.), методами топологического

анализа загрязнений Семипалатинского испытательного ядерного полигона (Макаренко Н. Г. и др.), приложениями символической динамики и алгоритмической сложности к геофизике (Терехов А. Г.), физикой столкновений в задаче необратимости (Сомсиков В. С.) и вычислительной геометрией (Кардашев Ф. В.). Интересные приложения методов детерминированного хаоса в криптографии инициировал сам Вильжан Мавлютинович; это направление стало весьма популярным в последующие годы. Идеи самоорганизации, которые появились в пионерских работах нобелевского лауреата Ильи Пригожина, развивали в задачах геологического моделирования В. Л. Лось и И. А. Гоберник. Нелинейные методы идентификации несанкционированных ядерных взрывов исследовались совместной группой из ИПТМ и ИГИ (Макаренко Н. Г., Беляшов Д. Н., Емельянова И. В. и др.). Напомню, что в 1990-е годы ядерные технологии активно развивались в Пакистане, который провёл ряд так называемых камуфлированных ядерных взрывов. Записи некоторые из них накладывались на частые в этом регионе землетрясения, так что задача их разделения была чрезвычайно сложной. Фрактальная геометрия и мультифрактальный анализ использовались в исследованиях по космологии (Макаренко Н. Г., Пушкарев О. А.). Проблеме прогноза уровня Каспия в рамках эмбедологии были посвящены исследования совместной группы геофизиков и математиков (Макаренко Н. Г., Каримова Л. М., Беляшов Д. Н., Тищенко А. В., Емельянова И. В. и др.). Идеи топологического вложения временных рядов использовались и для изучения вариаций общего содержания озона (Каримова Л. М., Иванов А. И.). Задачами малых деформаций в римановых пространствах занимался Азанов Н. П. из КГНУ им. Аль-Фараби. Диапазон перечисленных задач, их новизна и практическая направленность для стратегических планов Казахстана были полностью обусловлены талантом руководителя программы В. М. Амербаевым. Результаты были резюмированы в двух препринтах 1996 и 1997 гг., изданных под тем же названием, что и программа. Она послужила трамплином для защиты серии кандидатских диссертаций участниками семинара (Макаренко Н. Г., Каримова Л. М., Тищенко А. В., Мухамеджанова С. А., Круглун О. А. и др.).

Уже потом, спустя годы, я оценил мудрость нашего наставника. Вильжан Мавлютинович никогда не пытался привести нас к намеченной цели за оговорённое время. Напротив, его семинары походили на прогулки по саду, полному неожиданных и прекрасных растений. Прогулок, которые предусматривали остановки возле интересного объекта и возможность осмотреться в его окрестности.

В заключение расскажу о занятном эпизоде, связанном с моими собственными защитами: сперва кандидатской, потом докторской диссертации. Разумеется, всё нужно было делать вовремя, но получилось так, что у меня не было учёной степени до весьма зрелого возраста. И вот однажды Вильжан Мавлютинович вместе с Иваном Тимофеевичем Паком предложили мне заявить тему кандидатской диссертации, просто так, для включения в план, не предполагая реализации этого события. Я придумал *ad hoc* какое-то название, поверив, что это лишь пустая формальность. Не тут-то было! Спустя полчаса оба моих шефа с довольными физиономиями заявили мне, что диссертационный совет рекомендует к защите заявленную диссертацию и что у меня есть целых три дня, чтобы оформить её! Делать нечего, я попросил своих замечательных сотрудниц скомпилировать какой-то связный текст из различных моих публикаций, которых, к счастью, оказалось достаточно много и совсем из разных областей. Вильжан Мавлютинович просмотрел этот «*тришкин кафтан*» и заметил, что вообще-то для кандидатской диссертации достаточно трети из предложенного текста. После «*хирургии*» диссертация была успешно защищена, а дополненный вариант был использован для диссертации на соискание степени доктора технических наук по специальности 05.13.18, которую я защитил наконец в 2005 г. Следующая степень доктора была получена мной через год по физико-математическим наукам в Санкт-Петербургском университете.

Замечательным человеком был мой Наставник. Мы встречались с ним ещё раз после его отъезда, уже в Зеленограде, в его квартире. И тогда он с большим интересом обсуждал наши новые проблемы, научные и не только. Светлая ему память.

Образец Человека и Специалиста «высшей пробы»

Малашевич Б. М.
земляк, коллега, друг

Малашевич Борис Михайлович

С Вильжаном Мавлютиновичем Амербаевым мы дважды земляки.

Мы выросли в одном городе — в Алма-Ате. И там же получили образование. Он в КазГУ (математик), я в политехе (КазПТИ) по специальности «*математические счётно-решающие приборы и устройства*» (группа МСП-61, второй выпуск по этой специальности). Более двадцати лет ходили по одним улицам, возможно, и встречались, но судьба тогда нас не свела. Не было общих знакомых и общих интересов.

Свела она нас в Зеленограде, который для нас обоих стал второй родиной. Когда я в начале 1971 г. после окончания политеха, после двух лет работы на Загорском электромеханическом заводе и двух лет службы командиром взвода в Таманской дивизии поступил в Зеленоградский специализированный вычислительный центр (СВЦ), Вильжан Мавлютинович там работал уже шестой год.

До его перехода в 1972 г. в Алма-Ату я, конечно, знал о земляке — корифее в математике, а что он обо мне — весьма сомнительно. Старших инженеров было много, а наши сферы деятельности не соприкасались ни по сути, ни пространственно. Я (как представитель лаборатории главного конструктора) в то время участвовал в испытаниях ячеек и блоков завершаемой в разработке модулярной супер-ЭВМ 5Э53. Он разрабатывал для неё и последующих проектов алгоритмы модулярной арифметики, построенные на основе СОК (непозиционной системы

счисления остаточных классов), добиваясь со схемотехниками их хорошей аппаратной реализации (он всегда стремился довести свои теоретические изыскания до удачной аппаратной реализации). Я — в основном в лаборатории типовых испытаний в отдельном зданьице в лесу, он — на третьем этаже корпуса «Ш», где размещались теоретики СВЦ.

Естественно, поскольку СОК в СВЦ тогда рассматривался как светлое настоящее и будущее фирмы и всей вычислительной техники, я усиленно изучал единственную тогда по СОК книгу И. Я. Акушского и Д. И. Юдицкого «*Машинная арифметика в остаточных классах*». Но практически безуспешно. Математик я оказался никудышный, хотя в алма-атинском политехе по дисциплине «*высшая математика*» имел *отлично* (у меня сохранился вкладыш в диплом с оценками). В первой трети книги всё было ясно, во второй — сгущающийся «*туман*», в третьей — сплошное непроглядное «*молоко*». Но в отличие от математика «*от бога*» Вильжана Мавлютиновича, КазГУ-шные пятёрки которого тоже «девальвировались» в аспирантуре Математического института им. В. А. Стеклова, я не стал исправлять дефект математического образования, т. к. аналогичный дефект обнаружился и в образовании по основной специальности. Им я и занялся.

А в 1972 г. наши пути разошлись на три тысячи километров. Правда, однажды, будучи в отпуске в Алма-Ате, я по просьбе И. Я. Акушского что-то передал Вильжану Мавлютиновичу, посетив его в Институте математики и механики. Институт располагался в известном мне здании (минутах в 15 пешком от нашего дома), имевшем общий двор с моей школой № 35. После этой встречи мы с Вильжаном Мавлютиновичем перешли в категорию знакомых: при встречах здоровались, обменивались дежурными фразами.

Вильжан Мавлютинович в Зеленограде был фигурой известной, вызывающей интерес, поэтому СВЦ-шная общественность чётко отслеживала его перемещения то в Алма-Ату, то обратно, его избрание членом-корреспондентом, затем академиком АН КазССР, получение им Госпремии СССР, выпуск монографий. Но контактов у меня с ним, общих интересов и дел

не было. Встречались мы с ним либо случайно на улице как соседи (жили в Зеленограде в соседних «*башнях*»), либо на регулярных встречах СВЦ-шников в дни памяти Д. И. Юдицкого.

3 марта 1998 г. исполнялось 40 лет Зеленограду, а 8 августа — 35 лет Центру микроэлектроники. Руководство города и центра решило отметить этот двойной юбилей выпуском специальной исторической книги. Готовить её часть о микроэлектронике было поручено учёному секретарю НТС центра В. Н. Сретенскому. Василий Николаевич предложил мне написать об истории создания зеленоградских микропроцессоров и ЭВМ (МП и ЭВМ). Основания для обращения у него были. Во-первых, я был весьма осведомлённым (начальник отраслевой лаборатории по координации разработок МП и ЭВМ в Минэлектронпроме СССР и со смежными ведомствами и член отраслевого совета главных конструкторов, главный конструктор по системной совместимости МП и ЭВМ). Во-вторых, к этому моменту я уже был «*широко известным в узких кругах писателем*» — имел более 40 публикаций по профессиональной деятельности. Но я тогда отказался, считая, что для этого есть более статусные товарищи, да и художественным писательством я тогда заниматься не собирался.

Книга «*Зеленоград в воспоминаниях*» вышла, в целом хорошая, но об МП и ЭВМ в ней было очень мало и весьма путанно. Я пожалел, что излишне поскромничал.

Не сразу, но постепенно, оглядевшись вокруг, я пришёл к выводу, что кроме меня комплексно об истории МП и ЭВМ Минэлектронпрома написать некому. А в появляющихся публикациях увидел массу несуразиц. И я начал писать о том, что знал, что мог почерпнуть у коллег, в архивах центра, тогда ещё доступных. Постепенно у меня сложилась довольно толстая книга, со множеством очевидных нестыковок и противоречий, требующих разрешения. Этой «*утряской*» я занимаюсь до сих пор. Это как ремонт, его нельзя закончить, его можно только остановить. Однажды, прочитав свои первые писания, я ужаснулся, сколько «*несуразиц*» я тогда написал «*из своей головы*», на основе своего тогдашнего понимания, до «*утряски*». Я понял, что выпускать такую книгу нельзя, и начал публиковать её наиболее отработанные части в журналах, главным из которых был

«*ЭЛЕКТРОНИКА: Наука, Технология, Бизнес*» РИЦ «*Техносфера*». В нём в 2004 г. и вышла первая историческая статья «*Разработка вычислительной техники в Зеленограде: неизвестные супер-ЭВМ*». Тогда они действительно были неизвестны общественности.

В своей работе я пользовался помощью многих специалистов Зеленограда и отрасли из своих обширных рабочих связей, непосредственных участников и свидетелей событий. Одним из активнейших моих экспертов стал Вильжан Мавлютинович Амербаев, существенно помогший мне разобраться с историей создания модулярной арифметики и модулярных ЭВМ в стране. Так у нас появилось общее дело, общие интересы, постоянные контакты, наше тесное сотрудничество, постепенно переросшее в тёплую дружбу.

На встрече СВЦ-шников 22.09.2004, посвящённой 75-летию Д. И. Юдицкого, в своём выступлении Вильжан отметил, что в следующем, 2005 г. исполнится 50 лет СОК — в 1955 г. была опубликована первая в мире статья его изобретателей чехов А. Свободы и М. Валаха о применении СОК в вычислительной технике. Они же в 1962 г. в Чехословакии создали первую в мире модулярную ЭВМ «ЭПОС» (на реле), а затем в 1965 г. третью — «ЭПОС-2» (на транзисторах). Вторая в мире модулярная ЭВМ Т340А (в серийном производстве К340А) была создана в НИИ-35 (НИИ дальней радиосвязи) в 1962–1963 гг. Д. И. Юдицким и И. Я. Акушским. Она осталась непревзойдённым мировым рекордсменом по производительности среди ЭВМ второго поколения (на транзисторах). Четвёртой должна была стать ЭВМ 5Э53 Д. И. Юдицкого в СВЦ (на первых микросхемах), тоже мировой рекордсмен по производительности, в её разработке важнейшую роль сыграл Вильжан. Но её освоение в производстве на загорском заводе было остановлено в связи с прекращением работ по системе ПРО «Аргунь», для которой она создавалась.

К этому времени мой сын Денис закончил МИЭТ (по специальности «*системы автоматизированного проектирования БИС*»), поступил на работу в один из разрабатывающих микросхемы дизайн-центров Зеленограда и в заочную аспирантуру МИЭТ. Но с темой образовались проблемы. Его формальный руководитель от аспирантуры оказался слишком формальным

и ничего перспективного для защиты не предложил. В фирме по месту работы сына научная деятельность не поощрялась, а по тематике предприятия запрещалась. Т.е. нужно было выкручиваться самому. В связи с этим у меня ещё во время выступления Вильжана родилась мысль собрать на конференцию всех «*соковаров*» (так их называли в СВЦ, но Вильжан не любил этого названия, проводя аналогию с «*пивоварами*», поэтому более этот термин я применять не буду), с тем, чтобы разобраться в состоянии дел по СОК в стране и найти фирму, заинтересованную в разработке и применении модулярных микросхем (эта задача соответствовала и моим служебным обязанностям тогда уже в ОАО «Ангстрем», связанным с формированием портфеля заказов). Делать диссертацию на тему, в которой никто не заинтересован, я считал бесперспективным.

Я тут же изложил идею Вильжану, он её с воодушевлением воспринял.

Работа по организации конференции оказалась весьма трудной и длительной. Завершилась она выпуском сборника трудов «*Юбилейной Международной научно-технической конференции «50 лет модулярной арифметике*» (приведён в монографиях Вильжана) и проведением самой конференции в МИЭТе 23–25 ноября 2005 г.

В 774-страничном сборнике трудов опубликовано 44 доклада 51 авторов из России, Казахстана, Белоруссии, Украины и США, а также библиография по тематике СОК, включающая 1336 публикаций. При подготовке этих трудов к изданию мне пришлось все их прочитать, отредактировать, задавая вопросы авторам и согласовывая с ними изменения. При этом я значительно больше узнал о модулярной арифметике. Но много «*тумана*» и «*молока*» осталось — я действительно не математик.

Однако основные мои задачи конференцией выполнены не были — заинтересованных в реальном создании и применении модулярных микросхем не обнаружилось.

Но с тех пор наши дружественные контакты с Вильжаном укрепились.

А мой взгляд направился в сторону Николая Петровича Брусенцова, главного конструктора разработанных в МГУ

Открытие юбилейной конференции по СОК

в 1960-х годах первых (и последних) в мире троичных ЭВМ «Сетунь» и «Сетунь-70». К 2003 г., продолжая работать в МГУ, он глубоко проработал основы троичной арифметики и трёхзначной логики (попутно реабилитировав Аристотеля, «*ошибки*» и «*парадоксы*» в философии которого оказались искажениями гностиков, не понявших Аристотеля). В связи с этим Николай Петрович решил попытать счастья и сделать троичную ЭВМ на основе микроэлектроники. Руководство МГУ вроде бы поддержало идею, а в Ленинграде нашлась заинтересованная фирма. Так в 2004 г. Н. П. Брусенцов появился в ОАО «Ангстрем», где я тогда работал, там мы с ним познакомились.

Нас особенно сблизила одинаковая судьба прежних разработок, наших модулярных и его троичных ЭВМ — несмотря на серьёзные их преимущества в широких классах задач, и те и другие были «*убиты*». То, что по полсотни комплектов троичной «Сетуни» и модулярной К340А прекрасно работали, роли не сыграло. Кстати, десять комплектов К340А работают и в наши дни (почти 50 лет) в РЛС «Дунай-3У» под г. Чеховым Московской обл.

Часто при встречах я рассказывал Николаю Петровичу о модулярной арифметике, в результате у него возникла мысль о целесообразности попытаться объединить преимущества троичности и модулярности. Вильжану идея понравилась, состоялся ряд встреч в «Ангстреме» и в МГУ. Однако в результате ухудшения здоровья Николая Петровича и отказа руководства МГУ от разработки троичной ЭВМ эти работы потихоньку затихли. Но Вильжан довольно глубоко вник в проблемы троичной арифметики и трёхзначной логики, что позволило ему быть официальным оппонентом кандидатской диссертации ученицы Н. П. Брусенцова — Юлии Сергеевны Владимировой.

В МГУ. Обсуждение путей построения троично-модулярной ЭВМ. Слева направо: Н. П. Брусенцов, П. Р. Машевич (директор по НИОКР и госзаказу ОАО «Ангстрем»), академик В. М. Амербаев, инженер Д. Б. Малашевич, 11.10.2005

21 октября 2010 г. ушёл из жизни глубоко уважаемый мною человек — Александр Анатольевич Васенков, много лет бывший главным инженером Зеленоградского центра микроэлектроники. Мой начальник и коллега по работе, с которым мы были единомышленниками в производственных и общественных делах (с его преемниками такого не было). Меня попросили

подумать, как издать подготовленную им статью «*Некоторые события из истории микроэлектроники*». Задача была не простая — 70 страниц текста. Для журнальной статьи очень много, для книги — мало. Резать статью не хотелось из моральных соображений (согласие автора не получить) и жалко было терять содержание. Статья была интересная и оригинальная.

После долгих раздумий я пришёл к мысли делать специальную персональную книгу, дополнив её другими статьями Александра Анатольевича, его биографией, библиографией, воспоминаниями о нём и т. п. Но если книга персональная, то почему только про него? Есть много людей в нашей профессии, достойных такой книги. И первым для меня кандидатом на книгу № 2 был Д. И. Юдицкий.

Поэтому книгу, которая была названа «*Александр Анатольевич Васенков*», я оформлял как первую из тогда же придуманной серии книг «*Созидатели отечественной электроники*» (СОЭ). Средства на издание книги выделил также глубоко уважающий Александра Анатольевича генеральный директор ЗАО «НТ МДТ» Виктор Александрович Быков. Книга вышла в 2010 г.

А когда я принялся за подготовку второй книги серии «СОЭ» о Д. И. Юдицком, у нас с Вильжаном, близким другом и соратником Юдицкого, появилось новое общее дело, укрепившее наши отношения.

Книга «*Давлет Исламович Юдицкий*» вышла в 2011 г. Средства на её издание выделил Владимир Григорьевич Сиренко — истинный СВЦ-шник, генеральный директор ОАО «НИИ «Субмикрон». Главу 1 книги «*Выдающийся главный конструктор*» написал В. М. Амербаев.

Затем, правда уже без участия Вильжана (он не был знаком с героями книг), вышли книги:

«*Михаил Александрович Карцев*» (друг, коллега и лояльный конкурент Юдицкого); лично Карцева я не знал, но прекрасно знаю его ученика и преемника на посту директора НИИ вычислительных комплексов — Юрия Васильевича Рогачёва, с которым мы книгу и делали),

«*Валентин Михайлович Пролейко*» — основатель и в течение 27 лет начальник Главного научно-технического управления

Минэлектронпрома СССР, мой начальник и единомышленник в годы, когда я занимался координацией разработок МП и ЭВМ в Минэлектронпроме и со смежными ведомствами СССР, и коллега позже, когда мы активно занимались популяризацией истории создания и развития отечественной электроники.

В. М. Амербаев и Б. М. Малашевич на презентации книги о Д. И. Юдицком, 22.09.2011 г., музей ОАО «Ангстрем»

И вот вышла пятая книга серии «СОЭ» — «*Вильжан Мавлютинович Амербаев*».

Она завершает мою программу-минимум в серии «СОЭ» — выпуск книг о четырёх особо уважаемых мною людях в профессии, с которыми меня свела судьба: о Д. И. Юдицком, А. А. Васенкове, В. М. Пролейко и В. М. Амербаеве.

В связи с этим передо мной встал вопрос, что далее делать с серией «СОЭ». Продолжать её — огромная, требующая месяцев непрерывного труда на каждую книгу работа. Проект некоммерческий — никто из авторов денег не получает, издаётся

Первые четыре книги серии «СОЭ»

на средства спонсоров и раздаётся бесплатно, т. е. всё на энтузиазме. Пока я работал в «Ангстреме», мои начальники генеральный директор В. Л. Дшхунян и его заместитель П. Р. Машевич (оба СВЦ-шники) поддерживали меня в этом деле, позволяли тратить на него часть рабочего времени. Теперь я на пенсии, для достойной жизни явно недостаточной. Нужен дополнительный заработок, нужно другое дело, и такое дело у меня есть, но работа над книгами «СОЭ» ему серьёзно мешает. Свою программу-минимум я завершил и даже перевыполнил. Поэтому выпуск книг серии «СОЭ» я сокращаю: завершаю те, что в заделе, и, скорее всего, новых книг начинать не буду. Но, считая идею «СОЭ» позитивной и достойной развития, я буду рад, если кто-то подхватит и продолжит выпуск новых книг о других «*замечательных электронщиках*», при необходимости я помогу. Необязательно браться за серию в целом. Можно выпускать отдельные книги в рамках общей серии, по желанию энтузиастов.

Но вернёмся к Вильжану. В 2009 г., готовя к изданию книгу «*50 лет отечественной микроэлектронике. Краткие основы и история развития*», я в ней отразил и всю известную мне тогда историю модулярной арифметики. Но мне не хватало современного её состояния и прогноза на будущее. И я попросил Вильжана написать об этом, он любезно согласился и выполнил, как всегда, своё обещание. Но, поскольку книга была в моноавторстве, я не мог вставить его текст отдельной статьёй, а вставил его в виде цитаты Вильжана, чем закрепил его авторство. Вот как это выглядело:

В качестве примера этой активизации рассмотрим работы по созданию нового направления модулярной арифметики — модулярной логарифметики, выполняемые в зеленоградском Институте проблем проектирования в микроэлектроники (ИППМ РАН) академиком В. М. Амербаевым. Информацию об этой работе любезно предоставил сам Вильжан Мавлютинович (рис. 5.66).

«Привлекательные структурные особенности модулярной арифметики — параллелизм и распределенность арифметических операций на уровне операндов, а также арифметичная самокоррекция, потенциально обуславливающие высокую производительность и надежность вычислений, оборачиваются...»

Начало цитаты в книге

В настоящем сборнике этот текст представлен в виде отдельной статьи В. М. Амербаева под названием «*Модулярная арифметика сегодня*». Под этим же названием она включена и в библиографию Вильжана. Кстати, он написал и предисловие к этой книге.

Последние годы, особенно во время его работы в ИППМ РАН и (по совместительству) в «АНКАД» и МИЭТе, ознаменовались мощным всплеском его научной активности. Это было видно по жизни, по его активности, по его настроению. И хорошо иллюстрирует распределение его публикаций по годам гистограмма, приведённая в библиографии настоящей книги. В основном это связано с его предшествующими серьёзными заделами по применению модулярной арифметики в системах криптозащиты информации и с развитием предложенного Вильжаном нового направления модулярной арифметики — модулярной логарифметики. В обоих направлениях его окружали молодые талантливые ученики, что его радовало, воодушевляло и смягчало трудности жизни.

В 2011 г. Вильжану перевалило за 80 лет. Здоровье уже серьёзно усложняло его жизнь. Ему уже тяжело было регулярно ходить на работу, тем более в три места (ИППМ РАН, «АНКАД» и МИЭТ), даже при полном понимании и лояльном отношении руководителей предприятий, высоко ценивших Вильжана Мавлютиновича, создавших ему свободный щадящий режим работы.

Минаев В.В., Малашевич Б.М., Амербаев В.М.

Амербаев В.М.

На 70-летии Б. М. Малашевича, 23 июня 2010 г.

А ему приходилось решать дилемму.

С одной стороны, пора уходить «*на заслуженный отдых*». Но лучшим отдыхом для Вильжана всегда было занятие математикой. Он был из тех счастливых людей, для которых понятия «*профессия*» и «*хобби*» совпадали. Многие свои отпуска он проводил за этим любимым занятием, предпочитая его курортам и санаториям.

С другой стороны, жалко бросать новое дело на его взлёте. И жалко уходить от окружающей его талантливой молодёжи.

Эту дилемму он решал долго, понимая, что когда-то придётся уходить. Вопрос — когда? Он и дело себе нашёл для «*заслуженного отдыха*» — хотел систематизировать, упорядочить все свои наработки в области модулярной арифметики, чтобы создать крепкий комплексный научный фундамент молодым учёным, в которых он верил. А это огромная работа.

И, как рассказывает его супруга Эмилия Нестеровна, Вильжан уже решил, что пора, что время настало. И собирался в начале 2015 г. оставить активную, нормированную планами

предприятий работу в «АНКАД» и ИППМ РАН и заняться обобщением дела всей своей жизни в свободном режиме, в чисто домашних условиях, в тиши кабинета.

Но не успел. Судьба распорядилась иначе. 14 декабря 2014 г. его не стало. Не стало мгновенно, «на ходу».

Прошло уже четыре года, но его близкие, его друзья, его коллеги, его ученики не могут смириться с невосполнимой утратой.

Примером высокой оценки и любви к Вильжану Мавлютиновичу является решение двух его молодых учеников из ИППМ РАН Дмитрия Тельпухова и Екатерины Балака, награждённых президиумом РАН по итогам конкурса 2015 г. медалями РАН и денежными премиями[3].

Медаль РАН, которой награждены Д. Тельпухов и Е. Балака

Награду они посвятили своему учителю и наставнику — Вильжану Мавлютиновичу Амербаеву.

Ученики помнят Вильжана.

Все, его знавшие, помнят Вильжана.

Помнят с благодарностью и как пример для себя, для молодёжи, как образец Человека и Специалиста «высшей пробы».

---

[3] Награду они получили за научно-исследовательскую работу «*Разработка микроэлектронных устройств цифровой обработки сигналов с применением математического аппарата системы остаточных классов*».

Интервью, данное Д. Тельпуховым порталу *Zelenograd.ru*, помещено в настоящую книгу в разделе «*Публикации о В. М. Амербаеве*».

Мой Учитель — Вильжан Мавлютинович

Маткаримов Б. Т.,
д. т. н., в. н. с.,
Астана, Назарбаев университет

Маткаримов
Бахыт Турганбаевич

С Вильжаном Мавлютиновичем Амербаевым меня познакомил его друг и коллега Иван Тимофеевич Пак в начале 2000-х годов. Незадолго до этого я прочитал их совместную книгу «*Параллельные вычисления в комплексной плоскости*». Кроме того, в то время я активно занимался подготовкой школьников и студентов в области спортивного программирования, по существу это искусство программирования с акцентом на быстрой разработке и реализации алгоритмов для решения задач олимпиадного типа. Мы поговорили о текущих научных работах, и Вильжан Мавлютинович рассказал мне об особенностях машинной реализации модулярной арифметики. Меня до сих пор волнует вопрос, почему у нас не выпускаются лучшие в мире процессоры, и в той беседе я понял, что, с одной стороны, талант разработки алгоритмов может быть полезен в проектировании цифровых устройств, но, с другой стороны, этого совсем не достаточно, чтобы устройство увидело свет.

Впоследствии я предложил проект создания дизайн-центра проектирования цифровой электроники с использованием шаттлов для выпуска опытных образцов. В конечном счёте этот проект не реализовался, но эта тематика привела меня к активной работе с Вильжаном Мавлютиновичем. Мы занимались вопросами цифровой обработки данных, в том числе временных рядов, и вопросами модулярной логарифмической

арифметики, я многому научился у него, и эти знания мне существенно пригодились.

Вильжан Мавлютинович активно занимался наукой, его знания и мастерство позволяли заниматься фундаментальными задачами. Я не слышал от него фразы «*Зри в корень*», но именно так воспринимал его подход. Достаточно было поговорить с ним несколько минут и понять, что «*технические*» науки на самом деле «*фундаментальные*». Он много работал с учениками и публиковался: например, в 2009 году опубликованы три патента, с 2009 года — более 20 статей, на последнем году жизни — четыре журнальные статьи — это достойно восхищения!

Вильжан Мавлютинович стал моим консультантом по диссертации на степень доктора технических наук. Интересно отметить, что в диссертации была глава о тождествах для двумерного оператора Лапласа — Бельтрами (они содержат 864 и более членов), которые я получил совместно с Аскаром Серкуловичем Джумадильдаевым (используя модулярную арифметику), и Вильжан Мавлютинович уделил значительное время их изучению. Он не был ограничен своей научной тематикой и живо интересовался математикой в её полном разнообразии.

В Институте математики, г. Алма-Ата, 2010 г.

Одними из наиболее ярких моих воспоминаний о Вильжане Мавлютиновиче являются посещения его кабинета в Институте проблем проектирования в микроэлектронике РАН, а именно то, что его кабинет был всегда полон молодых студентов и аспирантов, с которыми он непрерывно работал! Для себя я объяснял это тем, что после развала СССР в кадровом составе учёных и инженеров образовалась большая возрастная брешь, передача опыта между поколениями стала огромной проблемой и существует политика привлечения профессионалов на пенсии к работе. Но, оглядываясь назад и уже имея опыт работы с молодёжью, я думаю, что Вильжан Мавлютинович был просто уникальным человеком с уникальной работоспособностью и уникальной готовностью поделиться знаниями.

Вильжан Мавлютинович очень любил город, в котором вырос, Алма-Ата и вправду является жемчужиной среди белоснежных гор Заилийского Алатау. Приезжая в Алма-Ату, он всегда посещал любимые с детства места и могилы родственников, он искренне радовался тем частицам старой Алма-Аты, которые до сих пор сохранились, отмечая и дома, и деревья.

В последний раз я видел Вильжана Мавлютиновича в Зеленограде осенью 2013 года, он был полон новых идей и рассказывал о перспективных задачах в области модулярной арифметики с гиперкомплексными числами и возможных приложениях в цифровой обработке сигналов, об оптимизации и надёжности вычислений.

До последних дней своей жизни Вильжан Мавлютинович работал и помогал молодым учёным, он навечно останется в нашей памяти ярким примером настоящего Учителя!

Светлая Вам память, Вильжан Мавлютинович!

Пусть ум и порядочность опять будут в цене

Ниретина Н. В.,
канд. биол. наук, зам. гл. учёного секретаря президиума АН КазССР 1969–1994 гг.

Скромность замечательных людей, которая часто кажется нам поразительной, во многом объясняется именно тем, что они... редко думают о своём «я» и по праву чувствуют себя обыкновенными людьми.

Т. Манн

Ниретина Надежда Васильевна

Мой выбор такого названия статьи и эпиграфа к ней совершенно не случаен. Именно таким я, и не только я, воспринимала при общении и при его отсутствии красивого, обаятельного, всегда улыбающегося Вильжана Мавлютиновича Амербаева.

Не смею и не имею права повторять известные факты из его научной биографии, его звания, степени и награды, не будучи его коллегой, но хочу подчеркнуть, что главное звание на Земле — это Человек. Он это звание оправдывал полностью, являя собой интеллигентного, общительно-доброжелательного действительного члена той высокой Сатпаевской академии наук республики и руководителя-организатора всех уровней.

Выпускник лучшего вуза Казахстана, единственного Казахского госуниверситета (КазГУ) им. С. М. Кирова, пройдя аспирантуру в ведущем Математическом институте им. В. А. Стеклова АН СССР в Москве, он был с конца 1950-х годов связан

с нашей академией. Моё знакомство с Вильжаном Мавлютиновичем, более или менее тесное, было во времена его работы заместителем директора Института математики и механики АН КазССР в 1972–1978 гг. Он был среди родоначальников нового направления науки в Казахстане — кибернетики, включающей в себя информатику. Оно зарождалось в созданной К. И. Сатпаевым лаборатории машинной и вычислительной математики при президиуме АН КазССР. Когда я пришла в президиум в 1967 году, то под кабинетами президента и первого вице-президента в большом помещении располагалась эта лаборатория.

Помню первую свою экскурсию к таинственным машинам огромного размера БЭСМ-3М и др. Они угрожающе мигали, сверкали, трудно было представить, что они могут быстро считать, тем более что через два десятка лет могут превратиться в компьютеры. И очень отрадно, что в нашей академии наук получило развитие это прогрессивное направление при активном участии и большой роли Вильжана Мавлютиновича.

Подробно, достоверно об этом периоде зарождения и развития центра вычислительной техники впервые в АН КазССР написал активный участник всего этого таинства в своей исторической книге «*Пережитое*», 2007 г., мой давний и добрый друг по сей день Иван Тимофеевич Пак. Вильжана Мавлютиновича я представляла всегда только в паре с Иваном Тимофеевичем. Такой настоящей, многодесятилетней дружбе единомышленников, коллег, соратников можно только позавидовать. И бесконечно жаль, что она оборвалась.

Не знаю и не могу обсуждать вопрос о причине отъезда В. М. Амербаева в Москву на постоянную работу, который уже был тогда членкором нашей академии. Но, как известно, через 11 лет Вильжан Мавлютинович вернулся в родные пенаты на высокую должность академика-секретаря отделения физико-математических наук АН КазССР, имея опыт преподавательской работы по своей специальности в Московском институте электронной техники. Этот опыт ему, скромному, сверхинтеллигентному человеку, по-моему, очень пригодился и помогал руководить, организовывать уже не студентов, а членов академии наук, почтенных и почитаемых аксакалов.

Отделение физико-математических наук, имея первый номер среди пяти отделений академии, всегда было во многом первым и единственным. Когда я пришла в президиум АН КазССР, академиком-секретарём отделения был, по-моему, Неменов Л. М., но я запомнила крупного, почему-то всегда в чёрном, Константина Петровича Персидского. Он как будто дремал всегда, но вовремя и в точку задавал вопросы и давал оценку.

Академики-секретари отделения физико-математических наук почему-то сменялись часто: Персидский К. П., Пентковский М. В., Такибаев Ж. С., Неменов Л. М., Тайманов А. Д., Султангазин У. М. На смену вышеуказанным академикам-секретарям пришёл обаятельнейший человек, известный математик Орымбек Ахметбекович Жаутиков. Более 20 лет он руководил отделением. Менялись президенты, главные учёные секретари президиума, но он достойно вёл корабль математиков и физиков по сложному лабиринту академии наук. Он дружил со своим ровесником, моим учителем Темиром Байбусыновичем Дарканбаевым. Было приятно и поучительно смотреть на двух беседующих в кабинете Темира Байбусыновича. Спокойные, справедливые, самодостаточные руководители, они ушли со своих должностей добровольно в 77 лет, оставив о себе светлую память прекрасных руководителей, отдав преемникам сплочённые коллективы учёных институтов. На освободившееся место и был приглашён из Москвы 57-летний Вильжан Мавлютинович, тем более что президентом в это время стал У. М. Султангазин — математик, бывший директор Института математики и механики.

Как я помню, В. М. Амербаев никогда не терял творческих и дружеских связей с институтом — и в период первого переезда в Москву, и до последних дней. Поэтому он был всегда в поле зрения академии наук. Выбор был осознанный и достойный всех предшественников. Непростое отделение, соединяющее в себе и математиков, и физиков, и астрофизиков, оставалось на виду, имея большие научные достижения, прекрасные кадры, проводя крупные международные конференции и совещания. Вильжан Мавлютинович был на своём месте, но долго

порулить ему не удалось по независящим от него причинам. К этому времени, как мы помним, бывший огромный единый Союз поделился на суверенные государства. И, естественно, на новом этапе развития экономики, общества, науки были повышенные требования к науке и прежде всего к главному штабу академии наук республики.

Академики-секретари отделений НАН РК: Сулейменов Р. Б., Жубанов Б. А., Сыдыков Ж. С. и Амербаев В. М. с главным учёным секретарём президиума НАН РК Сагадиевым К. А. в (центре)

Бесконечные предложения президиуму академии наук по повышению роли науки в переходный период, собрания, совещания, вызовы президента академии к президенту РК и в правительство не давали ощутимых, удовлетворяющих власть результатов. Было ясно, что нужен новый глава науки. Повода освободить У. М. Султангазина не было, заявления о добровольном уходе он, вероятно, тоже не собирался писать. И тогда кто-то заинтересованный придумал такой вариант, который в конце концов через два года привёл к ликвидации Академии наук РК в её классическом виде. Мы и здесь были единственными и первыми среди академий наук стран СНГ. Суть состояла в том, что все члены президиума НАН РК подписали

коллективное письмо руководству страны и общему собранию о досрочном сложении своих полномочий членов президиума. Знаю, что многие не представляли, что их должности связаны именно с членством в президиуме, полагая, что останутся вице-президентами, академиками-секретарями отделений. Но всё было продумано значительно серьёзнее и с дальним прицелом. Подписав это письмо-заявление, они автоматически должны были освободить занимаемые должности.

Итак, 2 февраля 1994 года состоялась сессия общего собрания Национальной академии наук РК. В работе сессии принял участие и выступил президент Республики Казахстан Н. А. Назарбаев. Сессию открыл президент НАН РК академик НАН РК У. М. Султангазин. В своём коротком вступительном слове он пытался отметить главные итоги работы этого состава президиума за период 1988–1994 гг. Но не дали: все ждали развязки первой в почти 50-летней истории существования главного штаба науки Казахстана, интриги.

Общее собрание НАН РК, учитывая письменное обращение членов президиума НАН РК к общему собранию о досрочном сложении с себя полномочий в связи с выполнением задач по первому этапу реформирования академии наук, постановило согласиться с обращением академиков НАН РК: В. Н. Околовича, А. А. Абдулина, Ж. М. Абдильдина, И. О. Байтулина, Б. А. Жубанова, З. М. Мулдахметова, В. М. Амербаева, Ж. С. Сыдыкова, А. К. Кошанова, Б. В. Суворова, М. А. Алиева, С. М. Кожахметова, С. Т. Сулейменова, членов-корреспондентов НАН РК К. Т. Ташенова, К. А. Сагадиева, Ш. А. Болгожина о досрочном сложении полномочий. За активное участие в работе по сохранению целостности академии наук, кадрового потенциала, известных научных школ и направлений в условиях экономического кризиса бывшим членам президиума НАН РК объявили благодарность.

В результате тайного голосования впервые на альтернативной основе, о чем не говорилось в уставе НАН, президентом НАН РК был избран член-корреспондент НАН РК экономист К. А. Сагадиев, ректор КазгосАкадемиии управления РК. В конкурсе участвовали академики НАН РК

У. А. Джолдасбеков — механик, директор Института механики и машиноведения НАН РК и Е. Е. Ергожин — химик, директор Института химии НАН РК.

В результате этих «*манипуляций*» Вильжан Мавлютинович, как и все, в начале 1994 г. вернулся в свой родной институт, получивший новое название — *теоретической и прикладной математики* на должность ведущего научного сотрудника. Обращаю внимание — не главного научного сотрудника, что было бы достойно для него, имеющего огромный опыт работы, лауреата Госпремии СССР в области науки, находящегося в расцвете сил и здоровья. Неудивительно, что он вскоре уехал опять в Москву.

Таким образом, академия наук РК, институт, мы — коллеги, соратники и друзья, расстались с прекрасным человеком, большим учёным. Его редкие приезды в институт и мои встречи с ним на общих собраниях НАН РК были всегда радостными, как с близким по духу, уважаемым человеком. Его уход в мир иной в достаточно молодом возрасте болью отозвался в сердце каждого казахстанца, кто его знал, кто с ним общался. Факт, что я его не видела в последнее мгновение, даёт ощущение, что он с нами, просто в Москве и скоро приедет опять. Но, как писал Е. Евтушенко:

Таков закон безжалостной судьбы:
Не люди умирают, а миры.

И это правда — с уходом Вильжана Мавлютиновича большой мир академии наук стал меньше, но утешает то, что такие люди, учёные были и мы не только работали вместе с ними, но и дружили и дарили друг другу тепло и радость. Эти люди не просто были — они творили, создавали новые направления математической науки, возглавляя свою школу последователей. Вильжан Мавлютинович подготовил для казахстанской науки около 30 кандидатов и докторов наук. И естественно, что в том, что институт математики при нём стал родоначальником пяти новых институтов, есть огромная заслуга В. М. Амербаева как большого, авторитетного в масштабе СССР учёного, руководителя института, отделения физико-математических наук, члена президиума НАН РК.

В 1991 г. в связи с возросшим масштабом проводимых научных исследований и наличием высококвалифицированных кадров по соответствующим научным направлениям из института выделены институты: космических исследований, механики и машиноведения, проблем информатики и управления, прикладной математики (г. Караганда), а сам институт переименован в институт теоретической и прикладной математики НАН РК.

И сегодня в академии наук трудятся ученики и соратники Вильжана Мавлютиновича. Его ученики подготовили своих учеников. Появились новые члены хотя и республиканского общественного объединения, но НАН РК. Благодарные ученики и коллеги чтут память о В. М. Амербаеве, продолжая на новом этапе дела своих предшественников.

Слово о друге

Пак И. Т.,
д. т. н., профессор, академик
РАЕН, заслуженный деятель
науки и техники РК

Пак Иван Тимофеевич

Вильжан Амербаев был большим моим другом.

В далёкие послевоенные годы (1949 г.) мы с ним одновременно поступали в КазГУ им. Кирова на физико-математический факультет. С ним мы были из разных социальных сословий: я из крестьянской колхозной семьи, а Вильжан Мавлютинович — из городской интеллигентной семьи. Отец его был доцентом по математике, работал в этом же КазГУ. Надо сказать, что Вильжан Мавлютинович сразу выделялся среди всех студентов. С самой

первой нашей встречи мы сразу же стали относиться друг к другу с симпатией. Эта симпатия вскоре переросла в большую дружбу.

Вспоминается вступительный письменный экзамен по математике. Нас было трое из одного колхоза «Авангард», который находился в казахской глубинке, далеко от столицы — в Баксайском районе Гурьевской области. Письменный экзамен для нас, колхозников, оказался очень трудным. Учась в школе, мы даже не подозревали, что кроме школьных учебников есть другие задачники по математике, предназначенные специально для подготовки абитуриентов. Конечно же, наших знаний было недостаточно, чтобы решить сложные задачи, заданные на экзамене. С примерами справились быстро, а задачу с применением тригонометрии никак не могли осилить. Мы заметили двух видных парней, которые, запросто справившись со всеми заданиями, покинули аудиторию. После долгих «*мучений*», один из нас, считавшийся наиболее подготовленным, попросился выйти. В коридоре он обратился к этим парням за помощью, и они подсказали ход решения непреодолимой для нас задачи. Этого было достаточно, чтобы быстро справиться с её решением. Оказалось, один из парней был сыном известного профессора по математике Константина Петровича Персидского, а другой — сыном доцента по математике Маулена Оспановича Амербаева. Вот так я впервые столкнулся с Вильжаном, тогда мы звали его Вильжоном.

Все годы учёбы в университете Вильжан Мавлютинович учился только на *отлично*. В течение всех пяти лет был старостой группы и всегда пользовался большим уважением. Дружил со всеми ребятами, был открытым в общении и нисколько не «*воображал*», что в учёбе он на голову выше своих сокурсников. Особенно его дружелюбный характер проявился во время пребывания в лагере военной подготовки. В трудных условиях месячной лагерной жизни Вильжан, имея хорошую физическую подготовку в отличие от других, в частности и меня, всегда помогал всем, опекал их. Как он сам вспоминал, именно там зародилась наша дружба.

На отдыхе с семьёй друга
Пака И. Т., 1981 г.

Мы, как он часто говорил, дополняли друг друга. Мы дружили семьями. Во время его пребывания в Алма-Ате благодаря инициативе его прекрасной красавицы супруги Эмилии Нестеровны у нас организовалось семейное географическое общество с посещением в выходные дни окрестностей Алма-Аты. Каждый из членов семьи, главным образом наши дети, делали доклады об истории и географии посещаемых мест. Незабываемые впечатления у нас остались от путешествия на моем автомобиле из Алма-Аты до Борового с ночёвками и посещением исторических мест Талдыкургана, озера Алаколь, Семипалатинска, Павлодара, канала Иртыш — Караганда, Целинограда (ныне Астана)... А трёхнедельный отдых на берегу озера Котыр-Куль с купанием и походами за грибами, с проживанием в комфортных условиях в гостинице сельскохозяйственного техникума доставил нам массу удовольствий и самых тёплых ярких воспоминаний, особенно нашим детям, моему Андрею и младшей дочери Вильжана — Оле.

Вильжан Мавлютинович был неофициальным научным консультантом моей докторской диссертации, также он являлся неформальным научным руководителем кандидатской диссертации моей покойной супруги Ирины, которая выполняла работу по прикладной социологии с применением математических методов.

Мы наметили с Вильжаном Мавлютиновичем переиздать книгу «*Параллельные вычисления в комплексной области*» на английском языке в Канаде, уже была договорённость об этом

с тамошними профессорами. Планировалось её дополнить ещё одной главой о самокорректирующихся особенностях в комплексной области. Об этом мы говорили на последней встрече в начале октября 2014 года, за два месяца до его кончины.

Вильжан Мавлютинович очень любил Алма-Ату. В последний раз он был здесь в 2010 году. В последние три года каждый раз планировал приехать в Алма-Ату, но что-то всегда препятствовало. При последней встрече мы планировали, что он обязательно весной 2015 года приедет, но судьба распорядилась иначе. Он всегда переживал, что не может часто посещать могилы своих родителей.

В душе Вильжан Мавлютинович всегда оставался романтиком. Очень трогательно было наблюдать, как он всегда поклонялся и обнимал тот большой дуб, который растёт на углу улицы Фурманова и Джамбула, у которого он впервые поцеловал свою несравненную супругу Эмочку.

Вильжан Мавлютинович особо любил моего сына Андрея. Он по-отечески опекал, поддерживал его во время учёбы в Институте электронной техники в Зеленограде. И мой Андрей трепетно, с большим уважением и любовью относился к Вильжану Мавлютиновичу и Эмилии Нестеровне. Каждый раз во время пребывания в Алма-Ате Вильжан Мавлютинович либо с внучкой, либо с дочкой останавливался в большом доме Андрея.

Вильжан Мавлютинович никогда не отдыхал ни в санатории, ни в доме отдыха. Он считал, что занятия наукой — это отдых. Мне как-то удалось в бытность моего зам. президентства академии наук два раза вывезти его за границу. Один раз — в Китай, другой раз — на мою этническую Родину Корею. В последние годы мы с Андреем много раз приглашали Вильжана Мавлютиновича и Эмилию Нестеровну в Карловы Вары, где у Андрея имеется небольшая собственность в виде четырёх номеров в гостинице. Но поездка по какой-то причине все откладывалась...

Я потерял большого друга, мы всегда понимали друг друга с полуслова. У нас не было с ним недосказанных мыслей. Мы скучали друг по другу, часто перезванивались. Мы были

очень близки духовно. Особенно это чувствовалось в последние годы, хотя мы находились в разных городах, даже в разных странах.

Визит в Республику Корея, посещение Корейской федерации науки и технологий, 1991 г. Справа налево: академики Мукашев Б. Н., Султангазин У. М., Амербаев В. М. и др.

Вильжан Мавлютинович позиционировался прежде всего как профессионал-математик. Он обладал энциклопедическими знаниями, с успехом справлялся с задачами практического приложения своей теории к проектированию арифметических узлов в микроэлектронике.

Вильжан Мавлютинович, светлую память о тебе я буду хранить всегда.

Нам повезло работать с Вильжаном Мавлютиновичем

Панасенко С. П.,
заместитель генерального директора фирмы «АНКАД»

Панасенко Сергей Петрович

Я познакомился с Вильжаном Мавлютиновичем относительно недавно, но впервые услышал о нем от своего отца, Панасенко Петра Васильевича, более 20 лет назад, когда я ещё учился в институте. Отец отзывался о В. М. Амербаеве как об очень хорошем преподавателе, грамотном специалисте, а также интересном и отзывчивом человеке. Проработав несколько лет вместе с Вильжаном Мавлютиновичем, я полностью разделяю мнение своего отца об этом великом человеке.

Вильжан Мавлютинович пришёл на работу в фирму «АНКАД» в 2007 году. Наша компания проводила различные научно-исследовательские работы в области криптографии и обеспечения информационной безопасности практически со времён своего основания. И приход к нам такого масштабного эксперта значительно усилил данное направление.

Помимо непосредственного участия в выполняемых фирмой «АНКАД» НИОКР, Вильжан Мавлютинович привлекался нами к решению любых задач, требующих экспертных знаний в области криптографических алгоритмов и протоколов. Тем более что, обладая, во-первых, отзывчивостью и стремлением помочь коллегам, а во-вторых, заинтересованностью в детальном изучении новых направлений и решении новых проблем в данной области, Вильжан Мавлютинович весьма охотно помогал другим сотрудникам фирмы и никогда не делил работу на «*свою*» и «*чужую*».

Вильжан Мавлютинович обладал большим авторитетом у студентов и аспирантов Московского института электронной техники, в котором преподавал в течение нескольких десятилетий,

и Московской государственной академии делового администрирования. Немало состоявшихся сотрудников фирмы «АНКАД» попали на работу в нашу компанию благодаря Вильжану Мавлютиновичу, за которым, в силу его прекрасных человеческих качеств и глубочайших знаний, студенты и аспиранты буквально тянулись. Отмечу, что Вильжан Мавлютинович стремился к тому, чтобы обучение его дисциплинам было максимально интересным для студентов. Достаточно часто, например, он советовался с коллегами по работе в части формирования заданий на курсовые и дипломные работы, с тем чтобы они отражали наиболее современный уровень науки и техники в данной области. Студентам давались задачи, относящиеся к известным и актуальным алгоритмам шифрования или хеширования, криптографическим протоколам, методам криптоанализа и т. п. Без каких-либо сомнений можно утверждать, что В. М. Амербаев вырастил целую плеяду специалистов в области криптографии, которые сейчас активно продолжают в том числе начатые им исследования.

За относительно недолгое время работы в фирме «АНКАД» Вильжан Мавлютинович успешно участвовал в ряде научно-исследовательских работ. Он был активным членом научно-технического совета фирмы, выпустил множество публикаций в соавторстве с другими специалистами нашей компании (в частности с Е. М. Зверевым, И. Е. Любушкиной, А. В. Шарамком, Д. Н. Тюфякиным), стал одним из авторов нескольких патентов фирмы.

И в том, что не касалось напрямую нашей работы, с Вильжаном Мавлютиновичем было весьма приятно общаться. Он проявлял живое участие в жизни коллег, интересовался их здоровьем, делами, успехами. Думаю, что не было ни одного человека в нашей компании, кто был бы не рад пообщаться с Вильжаном Мавлютиновичем. Многим из нас он запомнился в свой последний рабочий день, 12 декабря 2014 года, жизнерадостным и общительным, с доброй улыбкой на лице.

Считаю, что выражу общее мнение моих коллег, сказав, что нам всем весьма повезло работать вместе с Вильжаном Мавлютиновичем. Нам, благодаря его неоценимой помощи, удалось многое сделать и многому научиться. Жаль только, что это было так недолго.

Человек и Учёный с большой буквы

Семенов М. Ю.,
к. т. н., в 2004–2006 гг.
гл. специалист ИППМ РАН

Семёнов Михаил Юрьевич

В начале 2000-х годов в ИППМ РАН проводился ряд НИР по исследованию и разработке методов синтеза быстродействующих арифметических устройств. В ходе данных работ рассматривались также вопросы применения аппарата модулярной арифметики в системах цифровой обработки сигналов в больших динамических диапазонах для их реализации именно в интегральном исполнении. Мой научный руководитель, тогда ещё член-корреспондент, а ныне академик РАН Александр Леонидович Стемпковский посоветовал мне обратиться к эксперту по вопросам модулярной арифметики д. т. н., профессору Амербаеву Вильжану Мавлютиновичу, академику НАН Республики Казахстан. Так началось моё знакомство с этим замечательным человеком.

С первых минут я почувствовал его открытость и доброжелательность в общении. Если была какая-то срочная необходимость, Вильжан Мавлютинович без проблем приглашал проконсультироваться к себе домой. Я также увидел его громаднейший опыт и знания, которые он всегда стремился бескорыстно передать молодым специалистам: с одной стороны, очень спокойные и аргументированные объяснения, без какого-либо повышения голоса, а с другой — умение слушать и понимать собеседника.

Мне посчастливилось поработать с Вильжаном Мавлютиновичем лишь несколько лет, в период с 2004 до 2006 гг. Тогда же, в 2005 году, он согласился быть официальным оппонентом моей кандидатской диссертации, что накладывало на меня дополнительную ответственность, и я надеюсь, что не подвёл его. В моей памяти Вильжан Мавлютинович Амербаев всегда оставался и будет оставаться как Человек и Учёный с большой буквы.

Учитель с большой буквы, наставник и проводник

Тельпухов Д. В.,
ученик, нач. отдела ИППМ РАН

Тельпухов
Дмитрий Владимирович

Обычно днём памяти о человеке становится день его смерти, иногда день его рождения. Время, когда я вспоминаю Вильжана Мавлютиновича, не связано с этими датами. Каждую новогоднюю ночь с 31 декабря на 1 января, когда за окнами гремят праздничные салюты, а в квартирах открываются бутылки шампанского, я на время погружаюсь в воспоминания об этом замечательном человеке.

Первая наша встреча состоялась в 2008 году, и сказать, что это стало поворотным этапом в моей судьбе, — это не сказать ничего. Для меня Вильжан Мавлютинович стал Учителем с большой буквы, наставником и проводником. В то время, когда я стоял на распутье, искал своё место в жизни, Вильжан Мавлютинович показал мне красоту науки, величие и глубину математики, мягко направил и увлёк за собой. Всегда было приятно чувствовать себя в свете его научного

авторитета. Было приятно, и приятно до сих пор, считать себя учеником Амербаева. Я гордился и горжусь этим.

Но я перенял не только научные идеи. Его отношение к жизни и работе, вежливая манера общения с коллегами, мягкий стиль руководства, доверительное и местами наивное отношение к ученикам — все это очень сильно повлияло на меня. Главное, что меня всегда восхищало, — это то, что, несмотря на все заслуги, регалии, авторитет и высоту прожитых лет, Вильжан Мавлютинович никогда не позволял себе разговаривать свысока. Будь то нерадивый студент или признанный академик — со всеми он был вежлив, дружелюбен и внимателен. Его благородство и жизнелюбие стало для меня ориентиром в дальнейшей жизни и карьере.

Первый раз Вильжан Мавлютинович позвонил мне в Новый год в том же 2008 году. Звонок раздался почти сразу после боя курантов. Я был просто поражён. Я уже в точности не могу вспомнить, что именно мне пожелал Вильжан Мавлютинович, но я очень хорошо помню ту теплоту, с которой он меня поздравлял. Я был горд от того, что в новогоднюю ночь, в семейный праздник, мой научный руководитель вспомнил обо мне и решил сказать мне несколько тёплых слов. С тех пор каждый Новый год я ждал, и каждый раз после боя курантов неизменно раздавался телефонный звонок. И это было самое приятное и ожидаемое поздравление для меня.

С того времени изменилось многое — произошло множество событий и в личной жизни, и в профессиональной, сменился круг общения, поменялись научные интересы. Но главное — неизменным остался тот путь, который мне показал мой Учитель. И поэтому каждый Новый год, когда за окнами разрываются праздничные салюты, а в квартирах открываются бутылки шампанского, я с теплотой в душе вспоминаю Вильжана Мавлютиновича Амербаева.

Все его работы — результат больших трудов, отшлифованный до бриллианта

Тюфякин Д. Н.,
коллега по работе в фирме «АНКАД»

Тюфякин Дмитрий Николаевич

С Амербаевым Вильжаном Мавлютиновичем я познакомился в 2010 г. На тот момент я защитил диплом специалиста в МИЭТ и размышлял над продолжением своего обучения в аспирантуре. Вильжан Мавлютинович предложил поучаствовать в исследовании новой идеи организации шифросистем. Концепция ещё не была до конца сформирована, но уже тогда была смелой и амбициозной.

Работа была организована следующим образом. Мы делали некоторые предположения, основываясь на математике, затем проверяли их работоспособность на практике. Дорабатывалась программная модель и проводились статистические исследования. Анализируя полученные данные различными методами, мы корректировали нашу концепцию.

Очень скоро я понял, что, несмотря на диплом специалиста, моих познаний для исследовательской научной работы было недостаточно. Вильжан Мавлютинович почти каждую неделю приносил мне список книг по нужным направлениям математики, которые я изучал параллельно.

К программным моделям, которые мы использовали, предъявлялись повышенные требования по надёжности. Перед тем как сделать какой-нибудь вывод, все эмпирические результаты перепроверялись. Часто приходилось всё переделывать из-за неучтённой в модели «*мелочи*». Сначала я не понимал

такой организации и стремился быстрее двигаться дальше, как можно быстрее получить результат. Вильжан Мавлютинович каждый раз терпеливо меня выслушивал и убеждал не спешить, а делать все надёжно и обдуманно. Лишь спустя время я до конца осознал смысл такого подхода: полученные результаты ложились в основу дальнейших исследований и малейшая неточность могла увести нас от намеченных целей. Исследования становились всё объёмнее и объёмнее, а цена ошибки — всё больше и больше. Сбор статистических данных последней модели занял пять месяцев, а обработка — два дня. Если бы мы обнаружили неточность после получения результатов, то доверие к полученным данным было бы утеряно и пришлось бы начинать сначала.

Помню работу над нашей первой совместной статьёй. Она вышла в журнале «*Вестник МГАДА*» в 2013 году и называлась «*Симметричное шифрование в режиме пораундового сцепления. Статистический анализ стойкости*». Тогда мы решили опубликовать часть полученных результатов. Первая версия статьи появилась быстро, но работа над ней продолжалась всё доступное нам время. Когда мы первый раз отправили статью, редактор приняла её сразу, без замечаний. До выхода журнала оставалось время, и мы всё равно продолжили работу над статьёй. Редактор никак не могла понять, зачем мы ей присылаем всё новые и новые правки, если они и так сочли статью достаточно хорошей. Мы до последнего работали над статьёй, чтобы донести до читателя мысли по озвученной проблеме. В тексте не должно было быть ничего лишнего, чтобы не отвлекать читателя. Используемые слова должны быть взвешены, а материал по возможности опираться на другие исследования.

Все работы Вильжана Мавлютиновича есть результат больших трудов, отшлифованный до бриллианта.

С Вильжаном Мавлютиновичем мы плотно взаимодействовали почти четыре года. У него было много учеников и много работ, которые он вёл параллельно — с одинаковым интересом и упорством. На фирме, дома или в больнице, у него всегда был под рукой листок бумаги, карандаш и любимая математика. Он всегда работал. Был очень строг и требователен, но всегда

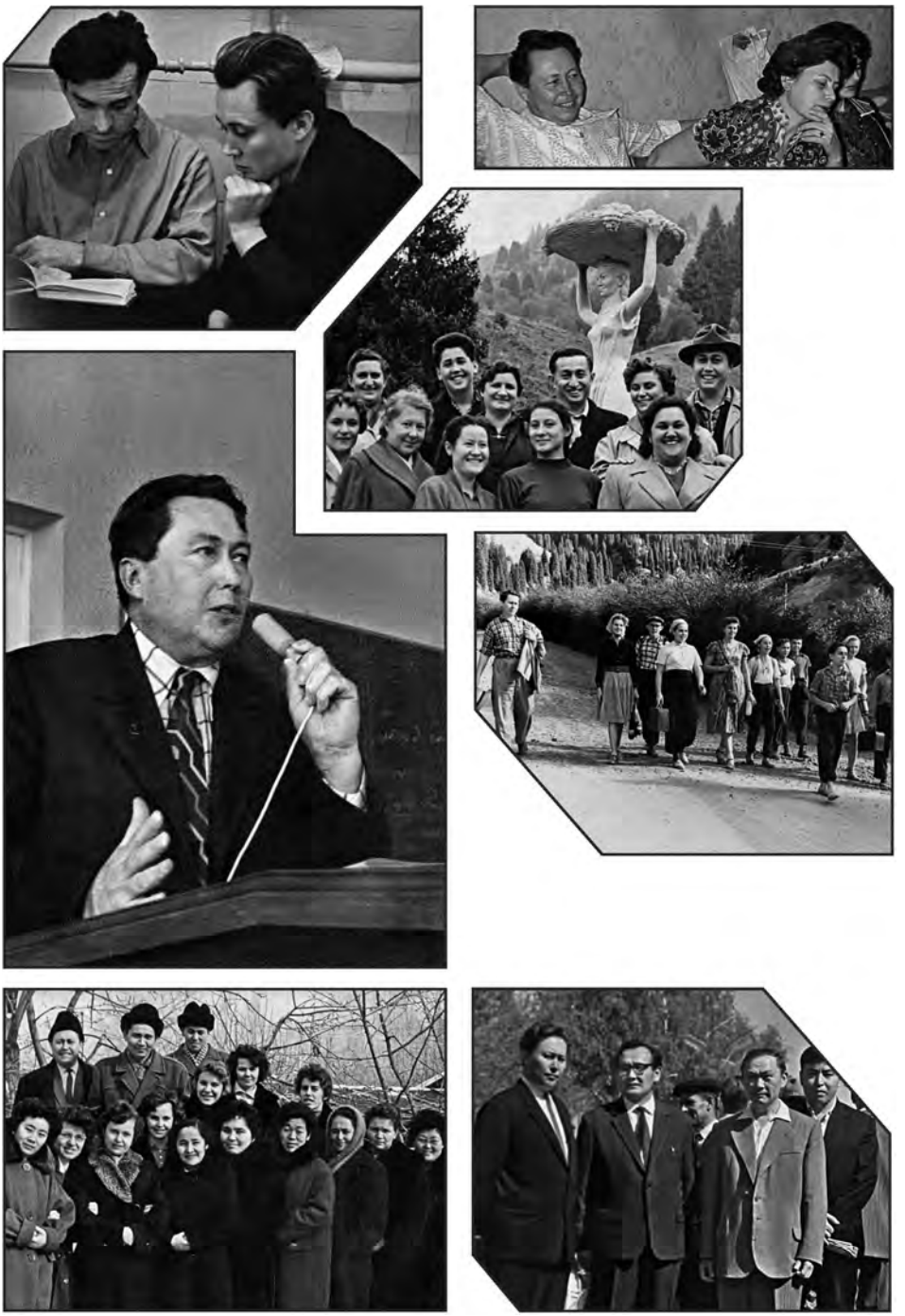
приветлив, старался помочь и объяснить. Наверное, этими качествами просто необходимо обладать, когда ты идёшь там, где ещё никто не ходил, идёшь для того, чтобы показать дорогу другим.

Я очень рад, что мне посчастливилось работать и учиться у Вильжана Мавлютиновича, и всегда буду его помнить как своего мудрого учителя.

Этими воспоминаниями мы заканчиваем книгу,
посвящённую широко известному и высокоавторитетному
в Союзе Советских Социалистических Республик,
в Российской Федерации
и в Республике Казахстан
выдающемуся математику,
внёсшему огромный вклад в создание и развитие
отечественной
вычислительной техники,
информатики,
систем защиты информации.

ВЕЧНАЯ ЕМУ ПАМЯТЬ!

Работа и отдых. *Вильжан с женой, друзьями и сослуживцами.*



Производство книг на заказ
Издательство «ТЕХНОСФЕРА»
125319, Москва, а/я 91
тел.: (495) 234-01-10
e-mail: knigi@technosphera.ru

СОЗИДАТЕЛИ ОТЕЧЕСТВЕННОЙ ЭЛЕКТРОНИКИ
Выпуск 5

Вильжан Мавлютинович Амербаев
Автор-составитель и редактор Малашевич Б.М.

Компьютерная верстка – ИП Автушенко Р.В.
Дизайн – Н.И. Семячкина
Ответственный за выпуск – С.А. Орлов

Подписано в печать 20.02.21
Формат 60x90/16
Гарнитура «Ньютон»

Печ. л. 35,5 п.л. Тираж 150 экз. Зак. № 1591
Бумага офсет № 1, плотность 80 г/м^2
Издательство «ТЕХНОСФЕРА»

Отпечатано в типографии ООО «Паблит»
Адрес: 127282, г. Москва ул. Полярная, 31В, стр. 1. Тел.: (495) 230-20-52
E-mail: info@publit.ru