УДК 929

Валерий Иванович Коржик: по дорогам, проторенным Шенноном, Финком и Вайнером

Коржик В. И.

“Главное, делайте всё с увлечением –
это страшно украшает жизнь.”
Л. Ландау

Актуальность. *В статье приводится описание научной и преподавательской деятельности доктора технических наук, профессора, Заслуженного работника Высшей Школы РФ, Почетного профессора Санкт-Петербургского государственного университете телекоммуникаций (СПбГУТ) им. М.А. Бонч Бруевича, постоянного члена международного общества IEEE on IT, Валерия Ивановича Коржика. Основные направления его научной деятельности это: теория сигналов, теория информации и помехоустойчивого кодирования, а также информационная безопасность, включающая в себя прикладную криптографию и стеганографию, в частности, так называемую, “бесключевую криптографию”. Преподавательская деятельность его делится на 25-летнюю службу в Военной академии связи и преподавание в СПбГУТ им. М.А. Бонч Бруевича с 1989 г. и до настоящего времени. Кроме того, он в течение трех с половиной лет работал по контракту в университете г. Мехико, а также читал курсы лекций, и занимался научной работой в 15-ти университетах Европы, Америки, Азии и Австралии. Результатом такой деятельности явилось написание около 200 печатных работ, включая 20 монографий и учебников, в том числе и на иностранных языках, а также подготовка около 50 инженеров и 38 кандидатов технических наук, 7 из которых впоследствии стали докторами наук и профессорами. В настоящей статье описываются также особенности обучения и преподавания в зарубежных университетах, некоторые природные условия и обычаи в странах, где ему пришлось работать.* ***Цель написания статьи*** *состояла в том, чтобы показать, что любой мотивированный и успешный российский ученый может сочетать посещение зарубежных стран с преподавательской и научной работой у себя на Родине. Для того, чтобы основное содержание не выглядело слишком сухим и скучным в текст статьи добавлены некоторые события из жизни автора.* ***Практическая значимость:*** *статья будет полезна молодым ученым, которые работают над проблемами в области теории сигналов, теории информации и помехоустойчивого кодирования, а также в областях прикладной криптографии и стеганографии, в плане постановки актуальных задач и примеров их успешного разрешения.*

Ключевые слова: *теория информации, концепция подслушивающего канала, криптография, стеганография.*

Введение

Я, Коржик Валерий Иванович, был удивлен, когда главный редактор журнала “Системы управления, связи и безопасности” С.И. Макаренко предложил мне написать в его журнале статью не по решению какой-либо научной проблемы, а описать мой путь в науке и образовании. Аргументировал он это тем, что начинающим исследователям очень важно увидеть “извилистый” путь

Библиографическая ссылка на статью:
Коржик В. И. Валерий Иванович Коржик: по дорогам, проторенным Шенноном, Финком и Вайнером // Системы управления, связи и безопасности. 2022. № 3. С. 314-381. DOI: 10.24412/2410-9916-2022-3-314-381

Reference for citation:
Korzhik V. I. Valery Korzhik: Along the ways paved by Shannon, Fink and Wyner. *Systems of Control, Communication and Security*, 2022, no. 3, pp. 314-381 (in Russian). DOI: 10.24412/2410-9916-2022-3-314-381

становления ученого, примеры успешного решения им творческих задач, узнать актуальность тех или иных направлений исследований, на взгляд уже состоявшегося специалиста в этой области, а также коснуться “закулисья” отечественной и зарубежной научной жизни. Ознакомившись с подобным примером статьи другого автора (проф. В.И. Левина), уже опубликованной раньше в этом журнале, я счел возможным согласиться. И вот, представляю такой мой “опус” читателям журнала. Замечу, что я часто старался избегать точных имен, упоминаемых мною в тексте персон, заменяя их начальными буквами имен или фамилии, чтобы не вызвать ненужных комментариев. Думаю, что такая “анонимизация” вполне допустима – ведь это не документ, а личные воспоминания. Правда, иногда я, все же, сохранял подлинные имена, если это казалось мне допустимым.

В.И. Коржик, 2021 г.

Отец мой, Коржик Иван Васильевич “из военнослужащих”, выбившихся в люди крестьян белорусского хутора “Кругляки” Слуцкого уезда. Благодаря своим способностям и трудолюбию, он в конце своей службы вышел в генералы и был заместителем Военной академии связи (ВАС) им. С.М. Буденного. Почти с первого и дольше последнего (когда он принимал капитуляцию немецких связистов Курляндской группы войск) дня войны, он воевал на Ленинградском фронте, будучи заместителем начальника связи фронта В.Н. Ковалева.

Моя мать, Коржик Фира Петровна (урожденная Феоктиста Зубова) происходила из мещан. Ее отец, то есть мой дед Зубов Петр Георгиевич, был приказчиком у известных чаеторговцев братьев Перловых. До замужества она работала в Наркомате обороны СССР, а во время войны (в эвакуации) – на свердловской станции переливания крови. После возвращения в Ленинград и после

рождения моей сестры, уже практически нигде не работала, находясь на иждивении мужа.

Отец, в 1938 г., во время “ежовщины”, был арестован, как “немецкий шпион”, готовивший покушение на самого … Сталина (!) и отсидел в Таганской тюрьме полтора года. К счастью, он не признался в этих вымышленных преступлениях и поэтому его не расстреляли, как произошло с его непосредственным начальником – районным военпредом и с начальником войск связи Рабоче-крестьянской красной армии (РККА) Лангвой. После выхода из тюрьмы и полной реабилитации (что иногда случалось с военными), он был направлен к новому месту службы преподавателем ВАС. На старом месте оставлять его, вроде, было неудобно – ведь на собрании сотрудников московского авиационного завода N 39, где он до ареста работал, уже гневно осудили его как вредителя, умышленно портившего военные радиостанции, хотя он раньше летал и с самим В.П. Чкаловым. Поэтому меня назвали Валерием не случайно. Так моя семья оказалась в Ленинграде (позже переименованным в Санкт-Петербург) и с этим городом была связана, в значительной степени, вся моя дальнейшая жизнь.

1. Ранние годы

Почти перед самым началом блокады Ленинграда, я с матерью эвакуировался в г. Свердловск, откуда мы вернулись в Ленинград после снятия блокады в 1944 г. В том же году я поступил в 117 мужскую среднюю школу, которую и закончил в 1954 г. с серебряной медалью. Во время учебы в 9-м классе я был избран секретарем школьной комсомольской организации, насчитывавшей около 300 комсомольцев. С большим энтузиазмом я занимался общественной работой. Даже как-то выступил на комсомольском активе Ленинграда в Таврическом дворце и поругал наших шефов из Всесоюзного института телевидения. Однако, в конце концов такая деятельность полностью меня разочаровала и в дальнейшем я больше никогда и никуда не выдвигался по комсомольско-партийной линии. Правда, я был рекомендован от Райкома ВЛКСМ для поступления в престижный московский ВУЗ – “Институт международных отношений”, как он тогда назывался, однако, посоветовавшись с родителями, я решил отказаться от этого предложения, в пользу инженерного образования, и поступил курсантом в ВАС на факультет радиосвязи. Закончил эту академию в 1959 г. С отличием и с золотой медалью и был направлен для дальнейшего прохождения службы (при собственном согласии, как тогда разрешалось медалистам) инженером в военный институт в г. Курске, где и проработал до 1962 г.

Поступив в ВАС, я был морально готов к любому месту дальнейшей работы, однако, во время обучения на старших курсах, уже пристрастился к “магии” научных исследований. В дипломной работе я разработал и сам собрал на стержневых лампах импульсно-кодовый модулятор. Сейчас это типовая микросхема аналогово-цифрового преобразователя (АЦП), но тогда мне казалось, что это научно-техническое достижение. Я даже во время стажировки специально ездил на завод в г. Новосибирске, где работал изобретатель этих стержневых ламп.

На последнем курсе ВАС мне присвоили звание сержанта, так как я, фактически исполнял обязанности помощника командира курсантского взвода. Поэтому я часто бывал вынужден заставлять моих подчиненных выполнять задания, в необходимости которых сам не был уверен. Причем, как и положено по воинскому уставу, без всякого объяснения необходимости их выполнения. Однако, я делал это без увлечения и поэтому получил прививку на всю мою оставшеюся жизнь – никогда не занимать позиции, которые требуют командования людьми.

После окончания ВАС, в Курске я занимался проблемой автоматического распознавания радиосигналов и даже получил за один предложенный мною метод свое первое авторское свидетельство, чем весьма гордился некоторое время. Будучи в Курске, я понял, что мне для успешной научной работы просто необходимо знание английского языка, тогда как в школе и в ВУЗе я изучал немецкий. Поэтому я взялся за это и нашел для помощи (и конечно не бесплатной) преподавателя английского из курского пединститута. (Замечу, что английский, как и в дальнейшем польский, определили и часть моей дальнейшей карьеры в науке и образовании). После трех лет работы в Курске я намеривался поступить в адъюнктуру при Военной артиллерийской академии в Москве, и там была даже предварительная договоренность с предполагаемым научным руководителем профессором М. Однако, не тут-то было! На медкомиссии военврач подполковник С. нашел у меня компенсированный порок сердца и никакие мои уговоры, что я де спортсмен и чемпион части по лыжам, а также просьба моих знакомых профессоров из курского мединститута, его не сломили-слышу шум в сердце и все тут. Пришлось мне перенаправиться в свой родной ВУЗ – ВАС, где я надеялся на не столь строгое отношение ко мне медицины. И уже после подачи моих документов в Ленинград, неожиданно вышел новый приказ с разрешением принимать в адъюнктуру с компенсированным пороком сердца. (Кстати, никогда после этого ни один врач не диагностировал у меня никакого порока). Однако, это событие можно рассматривать как “перст судьбы”, поскольку в ВАС моим научным руководителем стал д.т.н., профессор Лев Матвеевич Финк, с которым меня связала не только адъюнктура, но и вся моя дальнейшая совместная научная работа; просто это была радость находиться под влиянием такого ученого и человека, как Лев Матвеевич, вплоть до его смерти в 1988 г.

2. Научный руководитель. Начало научно-исследовательской и преподавательской работы в Военной академии связи

Мой научный руководитель, Лев Матвеевич Финк был в то время доктором технических наук, профессором ВАС, лауреатом Сталинской Премии, которую он получил еще во время Великой Отечественной Войны, находясь в группе, разработавшей, так называемую, “диверсионную помеху” для немецких пропагандистских передач. Она заключалась в том, что когда немецкие дикторы вещали по радио о грандиозных победах 3-го рейха, то на этой же частоте включались советские комментаторы, которые разоблачали угодливое вранье фашистских дикторов. Главный “пропагандон” Германии Геббельс был вне се-

бя от такой ситуации и требовал от немецких радиоинженеров, немедленно от нее избавиться. Однако, ничего не получалось и такое вещание продолжалось. Существовал даже миф, что, будто бы Гитлер назвал наших инженеров, создавших такую помеху, своими личными врагами и обещал их всех потом повесить, но и этого, к счастью, тоже не случилось...

Казалось бы, Льву Матвеевичу было вполне достаточно такого ореола славы для беззаботного существования в должности старшего преподавателя ВАС, но это, оказалось не так. Описание научной деятельности Льва Матвеевича заслуживает отдельной автобиографической книги. Скажу здесь лишь кратко, что общее направление его исследований это была теория электрической связи, в которой им основное внимание уделялось оптимальным методам приема сигналов, разнесенному приему и теории помехоустойчивых кодов, применяемых в различных каналах связи. Он написал первый в СССР полноценный учебник по общей теории связи и получившую большую известность монографию по теории передачи дискретных сообщений. Печатные труды Льва Матвеевича имели широкую известность в СССР, как и вся его научная школа, состоявшая из нескольких десятков адъюнктов и аспирантов, многие из которых стали потом профессорами и докторами наук. Что же касается известности его работ за рубежом, то хотя большинство его публикаций и были совершенно открытыми, но публикации в иностранных журналах у нас, мягко говоря, не поощрялись, особенно выполненные военными учеными. Правда, некоторые наши научно-технические журналы, такие, например, как “Электросвязь”, “Радиотехника”, “Проблемы передачи информации” и др. переводились на английский язык, но мало кто из иностранцев их читал. Некоторое окно (а скорее “форточку” в широкий мир) представляли собой международные конференции, проводившиеся в СССР (например, “Международный симпозиум по теории информации и кодированию”, “Всесоюзная конференция по теории кодирования”, на которые проезжали и многие известные западные ученые. Они проводились в таких привлекательных местах СССР как Дубна, Ташкент, Репино, Цахкадзор и поэтому тоже туда приезжали такие известные западные ученые как Е. Берлекэмп, Д. Мидлтон, М. Хеллман, Р. Галлагер, Т. Задэ и др. Дискуссии с иностранными специалистами, проводившиеся на платформах этих конференций, давали возможность, с одной стороны, показать достижения наших специалистов, а с другой стороны, быстрее и лучше ознакомиться с достижением западной науки в области теории информации и общей теории связи.

Кстати, остановимся немного на теории информации, создателем которой явился американский профессор Клод Эльвуд Шеннон. Думаю, что его роль в теории связи столь же велика, сколь роль А. Эйнштейна в физике. Конечно, сейчас это кажется очевидным, что для повышения надежности связи при наличии помех в канале, не обязательно снижать скорость передачи или уменьшать уровень помех, а возможно использовать лишь помехоустойчивое кодирование, если, конечно, пропускная способность канала больше скорости передачи сообщений. Само понятие пропускной способности канала связи с шумом было впервые введено и рассчитано для некоторых каналов связи, также К.Э. Шенноном. Заслугой Л.М. Финка явилось и то, что он без колебаний

принял концепцию Шеннона и внес в нее значительный вклад, вычисляя пропускные способности различных каналов (с замираниями, при разнесенном приеме и т.д.). Кстати, К.Э. Шеннон, посетил СССР и, в частности, институт Бонч-Бруевича, который тогда назывался Ленинградским электротехническим институтом связи (ЛЭИС) им. проф. М.А. Бонч-Бруевича, и читал там лекцию, причем, когда перевод делала преподавательница кафедры иностранных языков, то никто ничего не мог понять. И тут на сцену взобрался Лев Матвеевич и начал переводить да так, что сразу всем все стало совершенно ясно. Потом мы подошли с Финком к Шеннону и он подписал нам его книгу, недавно переведенную на русский язык (Я и сейчас храню ее, как ценную реликвию). К этому времени относится небольшой стишок, который я написал, прочитав работы Шеннона:

Когда б понять Шеннона смог и вникнуть в глубь его стремлений,
Я б в ресторане промотал получку всю без промедлений.
И над столом, подняв бокал, свободой выбора владея,
Я б ереванский пил коньяк за эти славные идеи!

(Историчность моих виршей подтверждается “ереванским коньяком”, поскольку тогда иного мы и не знали.) Еще хочу отметить одного столпа теории связи, но уже из России. Это академик В.А. Котельников с его “Потенциальной помехоустойчивостью”. Этот вклад в науку был признан во всем мире, хотя иногда и до сих пор попадаются изобретатели, которые приносят в научные журналы свои сверх оптимальные приемники. Опровержения многих таких “фейков”, как бы сейчас сказали, имеются в книге Л.М. Финка “Сигналы, помехи, ошибки”. Кстати замечу, что без теории Котельникова не было бы и информационной безопасности, так как тогда перехват уже расшифрованных сообщений, был бы возможен на любом расстоянии.

Говоря о роли научного руководителя в подготовке молодых ученых не могу не отметить одно мое наблюдение, что сейчас отношения аспирант – научный руководитель стали более формальными. Как ни странно звучит эта фраза, но они приобрели характер “оказания услуг”, тогда как в мои времена они носили более, я бы сказал, интимный характер. Это было постоянное общение, причем часто не только по научным вопросам диссертации, но иногда и по общим философским вопросам, часто связанным не только с наукой и обучением. Ученики Льва Матвеевича знали, что на любой наш вопрос всегда будет получен какой-то ответ. При этом он не пытался отослать тебя сразу же к какой-то книге или статье, но, взявши бумагу и ручку, начинал искать, хотя бы какое-то, наиболее простое решение “своим умом”. Конечно, бывали и такие трудные вопросы, на которые нам не удавалось сразу же получить ответа, но тогда мы, обычно уходили со встречным вопросом от Льва Матвеевича, ожидая ответа на свой сложный вопрос в ближайшем будущем. В качестве примера своеобразного отношения к своим аспирантам (адъюнктам в ВАС) могу привести, во-первых, мое стремление к изучению математики. Обучаясь в ВАС, я всегда чувствовал недостаточность образования в этой области. Поэтому ходил там на всякие дополнительные факультативы, например, на курс “Теории вероятностей”, читавшимся нашим доцентом Г.В.Е. Кстати, мы с моим приятелем и

однокашником записались тогда еще и в секцию самбо при Ленинградском доме офицеров, причем мне в качестве спаринг-партнера достался настоящий “амбал” под 100 кг весом при моем весе около 60 кг. После тренировок, когда он падал на меня всем своим телом, я чувствовал себя не очень комфортно. А на следующий день, как раз, и читался этот факультатив. Пришлось мне через месяц – два бросить самбо, тогда как мой приятель бросил факультатив. Впрочем, он лишь чуть позже меня защитил кандидатскую диссертацию, но, в конце концов, эмигрировал с семьей в США, где устроился на работу в одну частную компанию по … лужению.

Поступив в адъюнктуру, я одновременно записался и на курсы инженеров при матмехе Ленинградского государственного университета (ЛГУ) им. А.А. Жданова, хотя Лев Матвеевич и не поддерживал этот мой шаг, так как полагал, что те разделы математики, которые могут понадобиться для моей научной и учебной работы, я мог бы изучить и самостоятельно. Я же считал, что при таком сценарии всегда останусь недоучкой в области математики Мне хотелось и для своего даже удовольствия проникнуть в математику не поверхностно, и освоить не только основные ее результаты, но и технику доказательств вместе с аксиоматикой. Так что, в этом вопросе мы с Львом Матвеевичем разошлись во мнениях. Это, однако, не помешало мне успешно работать и дальше под его руководством. (Позже я перевелся на вечернее отделение матмеха и успешно защитился на красный диплом математика, выдав за него одну из своих работ, напечатанных в журнале “Проблемы передачи информации” АН СССР. Обучаясь на матмехе, я имел также удовольствие слушать лекции таких известных ученых и педагогов как Ю.В. Линник, З.И. Боревич, А.М. Вершик и др. что помогло мне и в дальнейшей моей преподавательской деятельности. С другой стороны, меня никогда не привлекала чистая математика, хотя один из моих преподавателей в ЛГУ (кстати ныне известный и на Западе профессор А.М.В.), даже предлагал мне поработать по одной из предложенных им тем, развивавших теорию операторов в Гильбертовых пространствах, но я благоразумно отказался – это было не мое; мне всегда хотелось видеть какие-то инженерные приложения математики. Интересно, что меня со временем, появился даже своеобразный подход – от математики к технике. В этом случае я просматривал какие-то математические методы, а потом искал для решения каких технических задач они могли бы пригодиться? Так изучая дифференциальные уравнения, я распространил понятие дискриминантной кривой на определение огибающей сигнала, которое является весьма важным для теории связи, а изучая понятие неполных сбалансированных блок схем в комбинаторике, нашел, что оно хорошо подходит для построения сетевых методов распределения ключевых данных.

Приведу еще один, казалось бы курьезный, случай моих университетских занятий. Дело в том. что на вечерние занятия в ЛГУ я обычно ездил из дома около часа, почти от кольца автобуса N 47. Забившись на заднее сиденье, я, от нечего делать, изучал самостоятельно, по самоучителю Д. Василевской, польский язык. (Стимулом для этого было чтение детективов на польском языке, которые тогда только и можно было купить в магазине “Демократическая кни-

га” на Невском проспекте). Тогда я еще, конечно, не знал, какую важную роль сыграет знание польского языка для моей дальнейшей работы и особенно в период “лихих девяностых” и о том, что много лет спустя, мы будем слушать концерт в Варшаве с моим знакомым, мужем (в то время уже, увы, вдовцом) автора этого самоучителя.

Первоначальной темой моей кандидатской диссертации было модное тогда исследование широкополосных сигналов для защиты от преднамеренных помех. На слуху была система связи “Фантом” и казалось, что она решит все проблемы защиты от таких помех, что было бы особенно важным для военной радиосвязи. Однако, как-то даже незаметно для самого себя, я съехал с этой темы и стал вплотную заниматься системами с обратной связью, использующими коды с обнаружением ошибок. Именно по этому направлению мне удалось опубликовать мои общепризнанные исследовательские работы. Еще значительное внимание я уделял построению моделей появления ошибок в каналах с замираниями. Помню, что самой первой моей печатной работой была статья, опубликованная в “Трудах Военной академии связи”, как раз по такой математической модели. Интересно также вспомнить, что идея этой работы пришла мне в голову не за письменным столом, а в комнате отдыха для народных дружинников, одним из которых я когда-то вдруг оказался. Чирикая что-то на случайном листочке бумаги, я понял, что количество ошибок различной кратности можно описать рекуррентной зависимостью.

Однако, главная моя работа в этом направлении была позже опубликована в общесоюзном журнале “Радиотехника” в 1965 г. причем я был весьма удивлен, когда приехавший из командировки в США профессор “Института проблем передачи информации” (ИППИ) М.С.П., сказал кому-то в ИППИ, что американцы называют полученную мною границу … “Неравенством Коржика”. Позднее я и сам нашел статью одного иностранного ученого с таким вот названием [1].

3. Докторская диссертация. Основная научная и учебная работа в Военной академии связи

После успешной защиты моей кандидатской диссертации в 1965 г., наступил наиболее приятный и успешный период в моей научной работе. Что же касается моей учебной работы, то ничего особенно выдающегося в ней тогда не было – я читал лекции и вел групповые занятия по курсу “Общей теории связи” под руководством Л.М. Финка. В этот период я совершенно не думал о подготовке докторской диссертации. В свободное от учебных занятий время ходил в научные залы Публичной библиотеки им. Салтыкова-Щедрина, где обычно читал интересующие меня научные статьи на русском и английском языках. (Если же в библиотечном буфете появлялись сосиски с зеленым горошком, то такой день казался особенно удачным). В этот период я довольно плодотворно публиковался в технических журналах по направлению теории сигналов и по использованию корректирующих кодов в каналах со случайными параметрами. Вспоминаю еще один стишок, который я написал в это время и по этому же поводу:

Ходит тигра цвета беш через джунгли Бангла-Деш,
Но охотник Чоудхури не стреляет тигру пулей.
За столом сидит он Рой-код придумал непростой,
В этом коде есть синдром, только где же Рой твой дом?
Ходит тигра цвета беш через джунгли Бангла-Деш,
Но охотник Чоудхури не стреляет тигру пулей…

(Напомню, что Рой Чоудхури был известным индийским ученым в области теории кодирования, одним из тех, кто предложил БЧХ код).

В то время, я был соавтором (с Л.М.Финком и др.) одного из первых в СССР учебников по “Общей теории связи”, изданного в ВАС. Замечу, что с написанием докторской диссертации меня никто особенно и не торопил, включая и моего научного руководителя, а также и моего начальника кафедры. Впервые я услышал подобный намек на одной из научных конференций от известного ученого в области статистической радиотехники Бориса Рувимовича Левина, который как-то при встрече сказал мне – как Вы еще не доктор? Тогда я впервые и задумался – а почему бы и не попробовать? В этот же период в Ленинграде функционировал научно-технический семинар по “статистической радиотехнике” в рамках научно-технического общества им. А.С. Попова. Руководителем этого постоянного семинара был Л.М. Финк, а позднее он передал мне бразды правления. На этом семинаре можно было любому желающему представлять свои новые результаты и проверять “на людях” их актуальность и правомочность. Вообще, считалось, что защищаться на степень кандидата и доктора технических наук в ЛЭИСе по кафедре Теоретических основ связи и радиотехники (ТОСиР), которую в то время возглавлял профессор А.М. Заездный, можно было только, пройдя этот представительный семинар. Так, не торопясь, я к 1972 г. подготовил свою докторскую диссертацию на тему “Помехоустойчивое кодирование в каналах со случайной структурой”, которая, в отличие от моей кандидатской диссертации, была полностью открытой и предполагалась к защите на диссертационном совете ЛЭИС. Почему же не в ВАС? Ну, во-первых, ничего особенно “военного” в ней не было, а, во-вторых, когда я как-то заикнулся начальнику научно-исследовательского отдела (НИО) ВАС, что хочу защищаться, то он, всплеснув рукам, воскликнул: “только не у нас!” Я был не против, понимая, что “пророков нет в своем отечестве” даже в узком смысле слова “отечество”. Защита прошла 22.06.1972 в ЛЭИСе, причем не из моего пижонства, а просто по случайности, у меня было не 3, как обычно требуется, а 4, оппонента. Среди них было 3 оппонента из Москвы, причем и такие известные ученые как М.С. Пинскер (из ИППИ). С.А. Самойленко (заместитель академика А.И. Берга в совете по кибернетике АН СССР) и Э.С. Блох – профессор, известный как раз своей моделью ошибок. “Против” проголосовало аж 4 члена диссертационного совета, хотя на все вопросы я ответил и отрицательных отзывов (из 25) у меня не было. Не знаю почему был такой счет, скорее всего, я был там “не свой” еще. Однако, счет оказался “проходным”, так что банкет, заказанный в ресторане “Баку” на Садовой улице, куда было приглашено аж 45 человек, прошел хорошо. (Правда, некоторые участники банкета явились к своим женам лишь под утро, оправдываясь тем, что, дескать, были раз-

ведены мосты…) Примерно через год (так было принято тогда по срокам) меня утвердил ВАК и я стал доктором технических наук (д.т.н.). (Как-то позже мне признался один профессор из Москвы, что именно он у меня был “черным оппонентом”, но написал на меня положительный отзыв). Профессора же в ВАС мне дали не почти сразу, как это было принято в ВУЗах, а через 6 лет, пока же я оставался д.т.н. и доцентом. Ну что же, опять вспоминается мудрость о пророках в своем отечестве.

Через пару лет после зашиты докторской диссертации, и по ее материалам, мы с Львом Матвеевичем издали монографию [2], которая, в народе получила название “Черной книги” (по цвету обложки), а несколько позже (1981 г.) я также с Л.М. Финком и с К.Н. Щелкуновым издали справочник по расчету помехоустойчивости [3], который был раскуплен через неделю после издания при тираже 15 000 экземпляров. Еще одна книга (совместно с В.В. Лосевым и Е. Бродской была издана в 1988 г. и была посвящена поиску и декодированию сложных сигналов. В этой книге были представлены, в основном, результаты моих соавторов, а моя роль состояла лишь в некоторых пояснениях и редактировании. Наконец, чтобы закончить с темой общения советских ученых между собой, отмечу, что все обстояло не так уж плохо. Регулярно проводились всесоюзные конференции по теории информации и кодированию, причем не в столицах, а в таких интересных городах, как в Ташкент, Ужгород, Киев, Севастополь, и конечно же, в Одессе. Особенно примечательными были зимние школы по теории кодирования, причем они проводились в таких местах, где в свободное от заседаний время, можно было покататься, да не на простых, а на горных лыжах. Это были: Цахкадзор, Бакуриани, Чимбулак. Еще одной знаменитой конференцией был, так называемый “Симпозиум по информационной избыточности”, который традиционно проходил на борту теплохода, плававшего по нашим Великим озерам (Ладожскому и Онежскому). На этой конференции складывались и свои внутренние традиции, например, при каждом таком круизе в городке Лодейное Поле, расположенном на берегу Свири, обычно проводился футбольный матч между “сборными командами” Ленинграда и Союза. На одном из таких матчей я даже был выбран капитаном ленинградской команды, но не как, конечно, лучший ее игрок, а как тот, кого знали все члены нашей команды. Правда, это знание нам не помогло и матч мы проиграли.

В больших городах ежегодно проводились конференции научно-технического общества радиотехники и связи им. А.С. Попова. Так что всегда существовала возможность и себя показать, и на других ученых посмотреть. Чтобы закончить с этой тематикой отмечу, что в 1995 г. в издательстве “Связь” был выпущен фундаментальный учебник, рекомендованный для всех ВУЗов связи СССР, который написали 4 профессора из СССР: А.Г. Зюко (Одесса), Д.Д. Кловский (Куйбышев), В.И. Коржик (Ленинград) и М.В. Назаров (Москва). Это был уникальный фолиант тиражом в 3000 экземпляров. “Да, вы нынешние – нутко” – можно сказать языком бессмертного “Горя от ума” теперешним авторам учебников, издаваемых каждым из университетов на свой лад.

Замечу, что лекционный курс “Общая теория связи” в ВАС гоняли с кафедры на кафедру, вместе с Л.М. Финком и со мной, но, наконец-то, меня при-

ютил один симпатичный начальник кафедры, которая изучала специальную технику, обеспечивающую безопасность военной связи. Пришлось мне от чистой теории связи переходить к изучению еще и безопасности связи. В этом смысле оказалось весьма кстати новое научное направление, разработанное A. Wyner-ом и опубликованное им в 1975 г. [4], которое мы называли "вайнеровской концепцией подслушивающего канала" или кратко – "каналом с отводом."

Фактически А. Вайнера можно было бы назвать "Шенноном информационной безопасности". Действительно, если Шеннон впервые установил предельную возможную скорость надежной передачи информации по каналу связи с помехами, то А. Вайнер впервые нашел максимальную скорость передачи информации, при которой по основному каналу легальных пользователей можно передать информацию абсолютно надежно, в то время как по отводному каналу (иначе по каналу перехвата), количество утекающей информации может быть сделано сколь угодно малой величиной. Эту максимальную скорость передачи по основному каналу он назвал "секретной пропускной способностью". Мне вместе с моими тогдашними адъюнктами, этот результат показался весьма актуальным для защиты систем связи от перехвата. С одним из них В.А.Я. мы напечатали работу по конструктивному расчету утечки информации в отводном канале и возможным методам кодирования в этом случае. Совершенно необычным в концепции Вайнера было то, что обычно корректирующие коды использовались в системах связи для исправления ошибок (то есть для повышения надежности), тогда как здесь – наоборот – для уменьшения надежности передачи по каналу перехвата, то есть фактически для его зашумления. Поэтому мы назвали такие коды "кодовым зашумлением". По данному направлению на нашей кафедре под моим руководством было написано и потом успешно защищено 4 кандидатских диссертации, а позже В.А.Я. защитил по этой теме и докторскую диссертацию. Было также получено несколько авторских свидетельств на изобретение и разработана практическая схема для защиты аппаратуры от побочных электромагнитных излучений при использовании данного метода, которая по договору была представлена одному московскому предприятию, но … грянул гром, то есть "лихие девяностые". В это же время я был научным руководителем ряда научно-исследовательских работ, выполнявшихся в интересах ряда московских предприятий, с целью обеспечения защиты систем радиосвязи от преднамеренных помех при помощи использования апериодических сигналов.

Примерно в то же время в научно-технической литературе появилась одна "прорывная работа" [5] по информационной безопасности, посвященная изобретению учеными из Стэнфордского университета В. Диффи и М. Хеллманом, "криптографии с открытым ключом". Мне представлялось данное направление весьма интересным и перспективным. Действительно, раньше казалось совершенно невозможным, как сейчас предлагали эти авторы, шифровать сообщения на одном ключе, а дешифровать – на совершенно другом, причем знание ключа шифрования не позволяло вычислить ключ дешифрования. Поэтому ключ шифрования можно было тогда сделать открытым (общедоступ-

ным) – отсюда и название данной криптосистемы, хотя точнее было бы называть ее “с открытым ключом шифрования”, но лишние слова убрали из определения и такое название непоправимо закрепилось. Много позже возникли всякие попытки доказать, что первыми в изобретении такой криптосистемы были англичане, но мол из соображений секретности, они не смогли опубликовать ее описание раньше, но как мне сказал один из авторов этого изобретения В. Диффи, с которым я неоднократно позже встречался на различных международных конференциях, этот приоритет англичан не подтвердился и именно В. Диффи и М. Хеллман позднее получили за это изобретение Золотую медаль имени Шеннона.

Конечно, не все в таком подходе было пока ясно. Ведь вычисление закрытого ключа по открытому сводилось к “трудной задаче математики”, например, к факторизации целых чисел. (Позднее появились подобные криптосистемы, основанные и на других трудных задачах –дискретного логарифмирования, коррекции ошибок линейными кодами и др.) Однако, точных границ для минимально возможного числа операций при решении этих трудных задач, пока не было найдено. С другой стороны, уж больно привлекательным казалось то свойство криптосистем с открытым ключом, что тогда не надо было заранее распределять ключи между пользователями, как в традиционных криптосистемах (называемых теперь симметричными). Достаточно было каждому пользователю самому сгенерировать свою пару ключей (шифрования и дешифрования), а затем по открытому каналу переслать своему корреспонденту ключ шифрования, на котором тот производил бы эту процедуру. Поэтому я решил через пару лет после появления этой идеи организовать семинар на нашей кафедре в ВАС с обсуждением перспектив применения таких криптосистем. Народу приехало много, причем, не только из Ленинграда, но также из Москвы и из других городов. После моего доклада было много вопросов, на некоторые из которых я попытался ответить, на некоторые – не смог. Однако, по окончании семинара один из его участников подошел ко мне и сказал “на ушко”, что у него имеются достоверные сведения, что использование таких криптосистем является тупиковым научным направлением, которое специально подброшено нам ЦРУ для введения в заблуждение советских ученых. Я пробовал возразить, что, конечно, тут есть много проблем, с которыми надо разбираться, но правомочность основных доказательств может быть легко проверена и не противоречит теории чисел, имеющей вековую историю. Так я этого товарища и не убедил в том, что этим надо заниматься. К сожалению, советские ученые не могли эффективно развивать теорию таких криптосистем из-за ограничений по публикации результатов в открытой печати, и мы потеряли порядка 10 лет, не занимаясь, практически, этим “тупиковым направлением”, в то время как на Западе оно эффективно развивалось и сейчас трудно себе представить без него обеспечение информационной безопасности, хотя бы даже только без применения цифровых подписей, использующих подобные несимметричные криптосистемы.

В 1976 г. в Ленинграде (точнее в поселке Репино под Ленинградом) состоялся международный симпозиум по теории информации, где мы представ-

ляли совместно с Л.М. Финком совместный доклад, правда, честно говоря, не вызвавший очень большого интереса. На этом симпозиуме присутствовало много известных зарубежных ученых в области теории информации, включая кодирование и обработку сигналов при наличии помех. Так там были М. Хеллман, Д. Мидлтон, Н. Слоан и многие другие. В тот раз мне не удалось лично познакомиться с изобретателями криптосистем с открытым ключом, но зато на банкете после окончания симпозиума я слегка к ним прикоснулся, поскольку … немного потанцевал с женой этого самого М. Хеллмана.

Вспоминая исследовательскую работу в ВАС, я как-то упустил свою основную там работу, а именно – обучение слушателей. Конечно, я читал курсы лекций по специальности. Проводил лабораторные работы и практические занятия (включая и полевые). Каждый год у меня было 3-5 дипломников и по несколько адъюнктов. Под моим руководством за этот период было выполнено и успешно защищено около 25 кандидатских диссертаций. Кроме того, я был консультантом по двум докторским диссертациям, участвовал в работе диссертационных советов ВАС, ЛЭИС и предприятия “Красная Заря”. Я также старался следовать этическим принципам Льва Матвеевича при работе с адъюнктами. Так в течение многих лет я снимал, как член Дома Ученых, на зиму государственную дачу в Комарово (пригород Ленинграда, где находится могила известной российской поэтессы Анны Ахматовой). Хотя моя дача представляла из себя всего лишь одну небольшую комнату с небольшой печкой в щитовом домике, но мы умудрялись иногда по средам устраивать там неформальные сборы адъюнктов, где они выступали с краткими докладами по темам своих диссертаций, причем часто в юмористической форме, а потом все шли кататься на лыжах около озера “Щучье”. Завершалось все это небольшим застольем с сухим вином и закусками.

Однако, не всё в моей работе в ВАС проходило так гладко. Так, начальник кафедры после моей защиты кандидатской диссертации (кстати, он был заслуженным профессором) говорил, что мне надо сейчас заняться больше методической работой, а исследованиями пусть занимаются те, которые еще не защитились. Наш заместитель начальника академии по учебной и научной работе очень любил меня отправлять каждые 4 года на войсковые стажировки в разные военные округа на пару месяцев. Один раз я был в учебном центре, находившимся в 40 км от Ташкента и обучал начальников радиостанций, в другой раз – оказался даже материально ответственным, главным инженером одного военного округа. Были и курьезные случаи. Так однажды начальник Войск связи СССР маршал Б., приехав в академию с какой-то проверкой, и проходя мимо стенда с фотографиями членов ученого совета, увидел мое фото со слишком длинными, как ему показалось, волосами. “Снять, постричь, сфотографировать и потом снова повесить” приказал он. Пока не повесили новое фото, меня мои знакомые спрашивали: “за что тебя сняли”, и мне приходилось каждый раз это объяснять. Меня дважды хотели отправить во Вьетнам, причем в первый раз еще во время войны, правда не в окопы, а преподавателем в военное училище. Первый раз я согласился (кстати, и по рекомендации моих родителей), но мое отправление отменили почему-то, а второй раз я не прошел уже по здоровью

медкомиссию. Еще одним испытанием для меня были военные игры, которые проводились у нас каждый год на зимних каникулах. Причем это не нравилось не только мне, поскольку все воинские и научные ранги там стирались и оставались только временные должности. Так однажды я выступал в роли коменданта понтонного батальона. Избежать этой игры не могли и маститые ученые. По этому случаю Л.М. Финк говорил в полушутку, что если бы ему предложили выбирать между военной игрой и сыпным тифом, то он бы еще подумал. Особенно неприятным всегда был финальный разбор игр, когда либо сам маршал, либо его помощники могли "повозить мордой об стол" любого доктора наук или даже какого-нибудь генерала. Еще одна неприятная обязанность работы в ВАС состояла в необходимости иногда дежурить по академии. Правда, при новом начальнике академии, деликатном П., доктора наук освобождались от обязанности дежурства по академии, иначе, проводя почти бессонную ночь, надо было еще проверять караулы и целостность знамени и денежного ящика с пистолетом на боку. В связи с таким дежурством, я вспомнил один случай, когда я еще был курсантом и стоял в карауле у спецкафедры с автоматом на ремне. Под утро пришла уборщица и стала убираться в охраняемой зоне, несмотря на все мои выкрики "Стой кто идет! Руки вверх!" и т.п. (в этом случае по караульному уставу полагалось стрелять сначала в воздух, а потом и в нарушителя…). Однако, к счастью для меня, и особенно для уборщицы, я не стал этого делать и просто вызвал разводящего. А так бы мог оказаться и … убийцей.

В 1988 г. произошло печальное событие-ушел из жизни мой учитель Лев Матвеевич Финк, выдающийся ученый с мировым именем, однако убранный перед этим с должности профессора ЛЭИС, поскольку его родственники уехали на постоянное место жительство (ПМЖ) в Израиль. Он был похоронен на Богословском кладбище Ленинграда, где несколько позже его семья и ученики установили ему памятник. Забыл сказать, что мой отец умер несколько раньше, в 1984 г. и был похоронен на Северном кладбище, где я несколько позже установил небольшой памятник из шокшинского камня, на котором было выбито разорванное кольцо-символ снятия блокады, в котором он непосредственно участвовал. Через 10 лет в той же могиле был захоронен и прах моей матери. Так что, с этого времени я остался круглым сиротой.

После смерти Л.М. Финка я первое время был в полной растерянности-кому я смогу задавать сейчас свои научные вопросы, кто сможет объективно оценить результаты моей работы и подсказать перспективные направления дальнейших научных исследований? Однако, надо было жить и работать дальше. Я не знал тогда, что меня, и по времени и по научным результатам, ждет еще "нижняя половина айсберга", если считать, что служба в Вооруженных силах (ВС) СССР, которой я отдал 35 лет, была верхней его половиной. Наконец-то, я смог реализовать свою мечту – демобилизоваться и устроиться простым профессором простого советского ВУЗа, скажем такого, как ЛЭИС. Мне в моем жизненном переустройстве помогло и то, что я не занимал никакой командной должности, будучи верным своему жизненному принципу, о котором уже писал раньше. Иначе бы меня стали удерживать дольше в военных кадрах. Ведь мне

было ... всего-то 54 года. Итак, с сентября 1989 г. я занял вожделенную должность профессора кафедры Теоретических основ связи и радиотехники (ТОСиР) учебного института ЛЭИС, который скоро стал университетом и получил наименование “СПбГУТ им. профессора М.А. Бонч-Бруевича”, сейчас, зачастую, более известный как “Бонч”.

Заканчивая описание первой части моей работы, а именно в ВС СССР, хотелось бы отметить напоследок еще некоторые приятные моменты, связанные с проведением зимних каникул и летних отпусков. Забыл упомянуть, что еще при обучении в адъюнктуре, я зимой съездил в Приэльбрусье покататься на горных лыжах. Условия, правда, были экстремальными. Во-первых, лыжи, которые я взял с собой, это были “Мукачи” – деревянные отечественные лыжи с укрепленной по краям внутренней железной полоской. (Почему-то я думал тогда, что сначала надо научиться кататься на таких деревяшках, а уж потом покупать зарубежный пластик). К горе Чегет мы приехали ночью – снега, горы, красота! Автобус остановился возле базы ЦДСА, на которую у меня была куплена путевка. К автобусу подошел начальник этой базы и с сильным кавказским акцентом сказал приехавшим горнолыжникам: “Условий никаких, каждый дэнь переломы”. После таких слов наш восторг природой несколько умалился, но большинство из нас, все же, осталось. На следующее утро пошли на Чегет, где нас встретил даже инструктор, правда, он проводил с нами не слишком много времени. К сожалению, через несколько дней такой жизни я на пустяковом склоне дернул себе мениск да так, что потом по утрам приходилось с трудом разгибать двумя руками забинтованное колено. Спать тоже было не очень комфортно – двухярусные койки в комнате человек на 40. Главное же было то, что такая жизнь не отбила у меня охоту кататься на слаломных лыжах, которые я позже купил уже из пластика и в ботинках “ботакс”. В другие зимы я катался на них в Цахкадзоре, в Чимбулаке, в Славске (и даже в Дивногорске под Красноярском) и вполне благополучно, то есть без особых травм.

В организованных турпоходах бывал трижды: по алтайским горам с заходом на Телецкое озеро и сплавом по реке Бие. Все было бы хорошо, но только мы шли с лошадью, которая опасно лягалась. Во второй раз ходил по Карпатам и для потехи прыгал с приятелем с мостика на плывущие плоты – хорошо, что они скоро сами выбросились на берег, и мы смогли догнать нашу группу. В третий раз я пристал к группе, проходившей по кавказским горам через Клухорский перевал с выходом в Чакви, где удалось даже погулять на греческой свадьбе. Несколько походов совершил вдвоем или в одиночку. С моим однокашником А. мы ходили по отрогам Памира вдоль речушки Каферниган и ночевали недалеко от поселка Рамит в виноградном саду, который охраняли два таджика. У меня было охотничье ружье с которым мы пытались поохотиться, так как все свои продукты уже съели. Мне удалось подстрелить только … дикообраза (“джайра” по-таджикски). Спросили у таджиков, можно ли его сварить? Они ответили: нам: “нельзя, но русские все съедят”. Вот мы сварили его и съели, а длинные иглы я привез домой для памяти.

В 70-х годах я решил в одиночестве прошвырнуться на Дальний восток и тому были веские причины. Во-первых, у меня был отпуск полтора месяца, как

и у всякого преподавателя, во-вторых, мне был положен бесплатный железнодорожный билет в купэ в любую точку СССР. В-третьих, мой отпускной билет разрешал мне допуск в любую погранзону. Итак, обменяв поездной билет на самолетный (с доплатой конечно), я полетел сначала в Хабаровск, потом на другом самолете на остров Сахалин, а потом еще на самолете в Южно-Курильск (на остров Кунашир) и оттуда на морском пассажирском корабле до Петропавловска Камчатского (на Камчатке). Далее, опять же на корабле до Усть-Камчатска и, наконец, на речном пароходике до поселка Ключи (под вулканом Ключевский). Не буду подробно описывать свое "небольшое" путешествие, но отмечу самые знаменательные его события. На Сахалине пошел в одиночный поход вдоль местной речки с парой ночевок в палатке у костра. Потом за мной пришли из турбазы и рекомендовали вернуться – уж больно было небезопасно идти в тоннеле деревьев и кустов вдоль речки, где были немалые шансы столкнуться лицом к … морде камчатского медведя, который тоже не дурак и ходит по эти тоннелям вдоль речек, а не ломится напропалую через берег, намертво заросший стланником. На острове Кунашир имел два привода на погранзаставу, но быстро отпущен как офицер Советской Армии, имевший разрешительный документ. На Кунашире был удивлен, что в местной столовой ел за 65 копеек горбушу с гарниром (по нашему-континентальному меню это казалось очень шикарно и дешево). Там же я напросился у капитана сейнера сходить с ним на ночную ловлю сайры. Это было феерическое зрелище, когда большая корзина невода освещалась цветными прожекторами с судна! Далее я намеревался на проходившем мимо пароходе доехать до знаменитых гейзеров в Жупаново и таки сел на этот довольно большой пассажирский корабль, но, увы из-за штормовой погоды он не смог выгрузить пассажиров на рейде Жупанова (а подойти к берегу он не мог из-за мели). И пришлось мне плыть на этом корабле дальше до Петропавловска-Камчатского. (Кстати, я уступил свое место в сетке для выхода на берег своему попутчику, ввиду того, что его намертво укачало.) Я тоже страдал от морской болезни, но не так сильно, хотя каждое движение в койке вызывало сильное желание воспользоваться специальным пакетом. На пароходе со мной плыл известный писатель Н.П. Задорнов ("Амур Батюшка" и др.) Он, почему-то, ко мне расположился и приглашал для разговоров в свою шикарную каюту. Перед расставанием он мне сказал, что принимал меня за тайного сотрудника КГБ, кем я, конечно, никогда не был. Приплыв в Петропавловск, я прожил там несколько дней и посетил со своими новыми приятелями Авачинской действующий вулкан. Вид на жерло вулкана был фантастическим, но спуск оказался для меня еще и пугающим. Надо было спускаться по крутому конусу без единого деревца или кустика метров 500. Казалось, что если споткнешься, то покатишься вниз безо всяких промежуточных остановок. Пришлось моим приятелям страховать меня на веревке до конца этого конуса. Наконец, я благополучно доплыл еще на одном корабле до Усть-Камчатска, где на речном пароходе еще несколько часов тащился до поселка Ключи. (В это время какие-то уголовного вида мужики в трюме играли в карты, и я не мог быть уверен, что не на мою персону). Ключи встретили меня фантастическим видом на вулкан Ключевский, но, конечно, забраться на него, во-первых, не

было разрешено, а, во-вторых, трудно было бы без специального снаряжения. Прождав несколько дней кукурузника который летал до Петропавловска, я, наконец, сел на него и вернувшись самолетом в Хабаровск, улетел домой на каком-то большом самолете. Можно ли было сказать, что так я летом “хулиганил”? (Одна моя знакомая девушка, с которой я, вместе со своим приятелем А. сдуру поехал в Крым, сказала мне, что она ко мне хорошо относится, но ей во мне не хватает … хулигана. Хотя я думаю, что хулиганом не был и мой приятель, к которому она во время нашей поездки вдруг расположилась. Через много лет я навестил ее в Одессе и не узнал из-за ее огромных размеров (а была-то тростинка)! Оказалось, что муж ее плавал на каком-то судне и оказался пьяницей (может это и эквивалентно хулигану?)

Наконец последний мой поход состоялся с моим однокашником по ВАС в Талышские горы (что расположены вдоль Иранской границы). Конечно, было и много других отпусков – в Крым, на Кавказ, в Прибалтику, в Карелию, по Золотому кольцу и т.д. Но ничего достойного внимания там не случалось, хотя все это было весело, приятно и просто замечательно. Да, широка страна моя родная и путешествуя по ней всегда можно напитаться настроением для всяких научных исследований в свободное от удовольствий время…

Помимо военных аспирантов (т.е. адъюнктов) у меня иногда проходили обучение и несколько гражданских аспирантов, в основном, из Узбекистана, причем за них мне никакие деньги не платили, и я их вел, как бы, для своего удовольствия. После успешной защиты, аспиранты, как привило, возвращались в свои южные края. Причем, поскольку благодарности на Востоке никто не отменял, то они приглашали воспользоваться этим восточным гостеприимством и приехать к ним в гости по тарифу “все включено”, т.е. предполагалась оплата перелета до Ташкента туда и обратно, проживание и питание за счет принимающей стороны. Правда, воспользовался я этим всего один раз, когда я вместе со своим приятелем, у которого также был на иждивении такой же неоплачиваемый аспирант, соблазнился и полетел в Хиву. Встреча была по высшему разряду, учитывая еще, что отец моего аспиранта оказался … районным прокурором. По прилете в Хиву, нас сразу пригласили в аэропортовский ресторан, где уже был накрыт стол с водкой. (Удовольствие это оказалось сомнительным – теплая водка при жаре в +40 градусов.) Но это еще полбеды. Хотелось отдохнуть после перелета и непривычной жары, но не тут-то было. Нас повезли к каким-то родственникам, где уже был накрыт дастархан с жирной едой и теплой водкой. Как-то мы это все перенесли и на ночь нас устроили в саду, причем в гамаках – чтобы “скорпионы не наползли” – объяснили нам. Ночь была душной, а, главное, истошно кричали ишаки. Нам объяснили, что у них сейчас какой-то гон, что-ли, и так ишачки требуют подать им своих ишаков, ну прямо сейчас. На утро, после осмотра достопримечательных мечетей бывшего хивинского ханства, мы поехали на машине километров за 100 в сад колхоза-миллионера, где, как нам рассказали, нас встретит мой аспирант и там опять же за столом, под которым протекает арык, мы отметим его успешную защиту диссертации. Все бы было хорошо, но дернуло меня отведать по дороге из грязного стакана придорожного продавца немного айрана (нечто из верблюжьего молока). Осталь-

ная часть поездки и вся ночь прошли в общении с оборудованием “прямого падения”. Потом мы сели (а я с трудом дополз до стола), который ломился от яств мясных, овощных и фруктовых, среди которых было и такое изысканное блюдо как перепелки, фаршированные молодым барашком, а я был вынужден пить только зеленый чай. Конечно, и эта напасть через пару дней прошла, но коронное блюдо я так и не попробовал. На востоке есть такое угощение пловом – “ашам”, когда твой “кунак” набирает в волосатую ладонь охапку плова и сует ее тебе в пасть. Отказаться нельзя. Это означает оскорбление гостеприимного хозяина. Так что с застольями на Востоке нужно быть всегда очень осторожным…

4. “Вторая жизнь” или работа в гражданском ВУЗе

Первое время я просто купался в счастье, что никто меня ничего не заставляет делать, чего бы мне совсем не хотелось, но потом попривык и все стало, так, как будто оно всегда у меня так и было. Однако, я надеялся на главное – стать “Человеком Мира”, то есть свободно перемещаться по всему миру, даже не придавая этому особого значения. Отмечу, конечно, что несмотря на некоторые негативные стороны моей службы в ВС СССР, я всегда чувствовал благодарность по отношению к государству и его представителям в лице моих преподавателей и учителей, которые обеспечили мне возможность получения высшего образования, а также научили навыкам научной и учебной работы, не говоря уже об обеспечении меня военной пенсией, что безусловно поддерживало материально меня и мою семью, позволяя более свободно заниматься научными исследованиями.

Вскоре состоялась моя первая командировка за границу, а именно в Белград (тогдашняя Югославия). Однако. она для меня не была особенно примечательной и типичной поскольку финансировалась нашим университетом, тогда как почти все мои последующие заграничные турне финансировались принимающими сторонами. В Белграде я обсуждал с югославскими партнерами (по договору с “Бончем”) вопросы построения и оптимизации модема для многочастотных систем связи КВ-диапазона.

Вот уже следующая моя поездка состоялась в Брайтон (Англия) на крупный научный форум Eurocrypt’91, где я делал совместный доклад с моим коллегой и приятелем профессором А.И. Туркиным из Горького (теперь это Нижний Новгород). Материал этого доклада был почти полностью разработан моим соавтором, а мне там принадлежала только математическая полировка и перевод материала на English. Название доклада было “Cryptanalysis of McElice Public Key Cryptosystem” [6], то есть “Взлом криптосистемы Мак Элиса”. Идея моего соавтора Туркина состояла в том, что поскольку криптоанализ криптосистемы Мак Элиса был известен, как трудная задача теории чисел, то он предложил погрузить дискретное пространство ключей в непрерывное, а затем решать в этом пространстве оптимизационную задачу; после чего-квантовать. Эту задачу, но в несколько упрощенном виде мы с Туркиным уже рассказывали на пароходе, плававшем по Великим Озерам и там на нас обрушился целый вал критики различных специалистов, но мы этот удар достойно выдержали. Наш

доклад в Англии имел весьма большой резонанс. Многие ученые подходили после него ко мне с вопросами и комментариями. Познакомили меня там и с автором взламываемой мной криптосистемы – самим Мак Элисом. К сожалению, дальнейший наш анализ этой работы показал, что хотя для ограниченных длин кодов этот алгоритм работал, но доказательство его полиномиальной сложности, в общем случае, не удалось получить. Поэтому в трудах этой конференции, хотя и был кратко описан наш метод, но отмечалось, что не все в нем доказано, как хотелось бы. В дальнейшем, я старался уговорить А.И. Туркина не пытаться доказать полиномиальность, а ограничиться лишь коррекцией ошибок для не слишком больших длин блоков. К сожалению, очень скоро мой соавтор умер от тяжелой болезни и, боясь, что кто-то украдет его идею, унес, как говорят, с собой в могилу все детали в общем-то примечательного алгоритма.

Положительным, для меня результатом этого симпозиума оказалось то, что там я познакомился со многими известными западными учеными в области открытой криптографии, такими как В. Диффи, Мак Вильямс, Х. Ван Тилборг, Д. Месси, Т. Клеве и другими. Эти личные знакомства существенно облегчили мне организацию дальнейших моих поездок в различные западные университеты для представления других моих результатов и проведения совместной научной работы. Однако, прежде чем перейти к описанию других моих заграничных визитов, которых в последующие годы набралось достаточно много, я хочу еще вспомнить одно важное событие, которое произошла в нашей стране в августе 1991 г. и в событиях которого мне удалось немного поучаствовать. Это, как известно, было выступление ГКЧП. Когда по радио “Балтика” мужчин Ленинграда призвали выйти на защиту Ленсовета от возможной атаки сторонников ГКЧП, я тоже решил присоединиться к ленинградцам, которые строили баррикады на улице, примыкавшей к Исаакиевскому собору. Для строительство баррикады мы использовали подручные средства, такие как, телеграфные столбы, автомобили и т.п. У нас даже была одна “жертва”, которую слегка пришибло упавшим телеграфным столбом. Меня руководитель строительства баррикады назначил для наблюдения в начале Невского проспекта за тем, не едут ли для нашего подавления десантники из Гарболова, которых, пока по слухам, назначил для этого дела командующий ленинградским военным округом. Нас учили также, сцепившись за руки, демонстрировать “гражданское неповиновение”. Однако, к счастью, ничего такого страшного не случилось, и причина этого была, конечно, не в нашем противостоянии ГКЧП, а в тех сотнях тысяч людей, которые вышли на улицы Москвы, демонстрируя этим свое несогласие с возвратом в бывший “совок”. Тем не менее, наш выход тоже был, хотя бы, моральной поддержкой москвичей. Однако, будучи всего лишь горсткой из нескольких тысяч людей на Исаакиевской площади, мы не знали в то время, чем для нас все это обернется, но были морально готовы ко всему, лишь бы не вернулось снова изучение краткого курса КПСС, включая и райкомовские проверки лояльности всех, кто собирался выезжать за границу (и не только это). Так мы провели целую ночь перед Мариинским дворцом, а утром к нам прибыл из Москвы А. Собчак и, выступив из окна первого этажа этого дворца, сообщил, что опас-

ность миновала, ГКЧП самораспустилось и мы тоже можем спокойно идти домой и ждать дальнейшего развития событий в демократическом направлении.

Мое личное знакомство на конференции в Англии с профессором Torleiv Klove из технического университета в г. Бергене (Норвегия), который, также как и я, занимался кодами с обнаружением ошибок, привело к тому, что в будущем году меня пригласили на два месяца как Visiting Professor в этот университет. Основная цель визита состояла в подготовке план-проспекта нашей общей книги, которую мой соавтор предложил издать в академическом издательстве Kluwer. Работу над этой книгой (на английском языке) я продолжил в Ленинграде в течение следующей пары лет, причем в 1994 г. я еще раз приезжал на месяц в Берген, чтобы окончательно согласовать с T. Klove некоторые ее разделы. В итоге, в 1995 г. эта наша книга вышла в том издательстве, о котором мы ранее договорились. Во время моего пребывания в Бергене я прочитал для местных аспирантов цикл лекций по кодированию в каналах с переменными параметрами, съездил (точнее слетал) в северный даже для Норвегии, университет Тронхейма, где прочитал лекцию о своем обобщенном алгоритме Витерби. Жил я в течение этих двух поездок в Бергене на кампусе универа, который назывался “Фантофт”. В выходные дни старался посмотреть, насколько это было возможно, прекрасную природу Норвегии. В частности, мой конфидент пригласил меня как-то в свой дом, расположенный над широким и лесистым фьордом, откуда открывался замечательный вид на океанские пароходы, проходившие по этому фьорду в порт Бергена. Сам город Берген (второй в Норвегии по величине после Осло) тоже очень живописен. В порту по воскресным дням открывался рыбный рынок, где продавались только что выловленные морепродукты включая и такую экзотику как осьминоги, кальмары, мидии и т.п. Рядом с портом находится исторический квартал с одно и двух этажными домиками будто бы рыбаков, но сейчас там находятся, в основном, сувенирные лавочки. В пригороде Бергена расположен дом композитора Э. Грига, а рядом с домом-бунгало, где стоит рояль Э. Грига, на котором он сочинял свою северную музыку, глядя через большое окно на открывающийся вид фьорда и кораблями на нем. В этом городе почти каждый год проводятся музыкальные фестивали Э. Грига, где и мне, однажды, удалось побывать и прослушать концерт российского композитора А. Шнитке для органа с оркестром, причем оркестр был в Бергене, а орган находился в Тронхейме. (Кстати это город, где всегда происходит коронация норвежских королей.) В Бергене много сирени (я как раз был там во время ее цветения – в мае), но почему-то она почти не пахнет? Мне, вроде, говорили, что селекционеры специально вывели такие непахучие сорта, чтобы избавить людей от аллергии. Неужели аллергия стоит запаха сирени?! Во время моего пребывания в Бергене, мне платили их профессорскую зарплату. Это позволило мне, вернувшись в Россию, купить небольшую бревенчатую дачу с 6-ти соточным участком на Карельском перешейке под Питером. Помимо дома на фьорде, мой знакомый профессор имел еще дачу километрах в ста от города. Ехать надо было на его машине по вершине гряды над фьордом. Вид на фьорд был совершенно потрясающий пока мы не заскакивали в один из 20 тоннелей, а общая длина этих тоннелей была, наверное, километров 50. Дом ока-

зался не слишком шикарным (бывший коровник), но вполне пригодным для жилья. Недалеко от дома (дачи) находился довольно высокий и мощный водопад, куда мы тоже совершали прогулки. На следующий по приезде день мы пошли в настоящий лес. Идя по тропке, я вдруг заметил, что вдоль нее рядами стоят грибы, а точнее говоря – подосиновики. На мой вопрос, почему же их не собирают, Торлеив ответил, что у них все грибы, кроме шампиньонов из магазина, считаются ядовитыми. Я, конечно, не мог снести такого грибного оскорбления и начал собирать их в снятый с себя плащ. Приволок целую охапку, почистил, потом отварил и мы их съели "за милую душу", причем никто не умер – знай наших! В 1993 г. меня пригласила профессор Дженнифер Себбери из Вол-лонгонгского (Австралия) университета на международную конференцию "Australia Crypt", которая и проходила тоже в Австралии, причем расходы на дальний перелет и проживание оплатила принимающая сторона. Так я оказался в Австралии на берегу Тихого океана. На этой конференции я делал свой доклад по тематике "Wie-tap channel". который должен был быть опубликован в трудах этой конференции. Правда, вместо того чтобы наслаждаться красотами Зеленого континента, мне пришлось довольно долго сидеть под вентилятором в своем бунгало на кампусе и править этот доклад. Город Сидней находится примерно в 40 километрах от кампуса и добраться туда можно было бы на электричке. После экскурсии по городу и прогулки под мостом на катере, я заранее условился встретиться с группой местных профессоров, которая тоже поехала в город. Однако, мой пароход опоздал на 15 минут. Пришлось мне прямо-таки бежать по незнакомому городу на место встречи и, все же, я опоздал минут на 5 к условленному времени. Однако, потолкавшись минут 15, я не увидел там никого из моих знакомых и пришлось мне пойти по городу в поисках вокзала для поездки на кампус. Тут я вдруг заметил, вроде, их автомобиль на одной из улиц, расположенной довольно далеко от назначенного места встречи. Посигналив рукой, я остановил машину – это были действительно они. Оказалось, что они точно подъехали к условленному месту встречи и не подождав ни одной минуты больше, покатили обратно на кампус, можно сказать, бросив меня в незнакомом городе и даже без точных сведений по поездам от вокзала. (Напомню, что мобильников тогда еще в обиходе не было.) Я подумал, что, приедь ко мне иностранец в Питер, я бы уже, наверное, не 5 минут, а час ждал бы его (её) на условленном месте. Ну что же – разная ментальность. Надо и к этому привыкать.

После окончания конференции профессор Себберри собиралась поехать на машине в Брисбейн – он находится примерно всего в тысяче километров к северу от Сиднея, и она обещала подхватить меня, поскольку мне было бы интересно проехать довольно большой кусок побережья Тихого океана и посмотреть тропический город Брисбейн, где меня обещали встретить в местном университете, а я должен был там тоже прочитать какую-то лекцию.

Поездка прошла без происшествий. Вообще-то Австралия это, в основном, пустыня, и только по краям континента находятся города и поселки с местными жителями, а кое-где живут и, так называемые, аборигены. При проезде по прибрежному шоссе нам иногда попадались сбитые ночью, в свете фар,

небольшие кенгурушки (конечно не те исполинские монстры, у которых в большей голове хватало ума не выскакивать на дорогу перед машинами ночью). Поселили меня в шикарном отеле Royal Garden. До этого времени я еще никогда не жил в таких дорогущих двухкомнатных апартаментах. Однако, ознакомиться с городом времени почти не было, так как я еще “причесывал” свой доклад на Австралия крипте и все самое красивое видел из окна отеля – это был тропический сад напротив. Заглянул потом и в зоологический сад, где посмотрел местную фауну.

В 1990-е годы меня несколько раз приглашали на криптошколу в немецком городке Dagschtuhle. Там мне удалось лично познакомиться с одним из разработчиков известной криптосистемы RSA А. Шамиром. Я показал ему мою компьютерную программу для демонстрации принципа вайнеровского метода кодирования в канале с отводом. Эта программа наглядно демонстрировала, как обычные, визуально представленные буквы, при выполнении кодового зашумления, могут быть лучше защищены от восстановления, причем, даже при небольшом уровне канального шума. Эту демонстрацию Ади Шамир посмотрел с неподдельным интересом. Вообще, я заметил, что иностранные ученые часто, хотя и, будто, проявляют заинтересованность, когда им рассказываешь какие-то свои результаты, но эта заинтересованность бывает лишь внешней, если только их научные интересы в точности (!) не совпадают с тем, что ты им демонстрируешь. (Правда, к А. Шамиру это замечание не относится. Его интересовали многие вопросы криптографии и защиты информации далеко за пределами криптосистемы RSA). Недалеко от Dagschtuhle оказались и австрийские города Klagenfurt и Linz, университеты которых, я посетил со своей лекцией по приглашению одного австрийского профессора. Заезжая в Австрию, нельзя было не заскочить в город Моцарта Зальцбург с его прекрасным видом на Альпы, фиакрами для туристов и домом Моцарта, который меня удивил своей миниатюрностью. Город Линц известен тем, что в нем когда-то Гитлер изучал искусство. Жаль, что он не достиг в живописи больших успехов – иначе бы, наверное, не было холокоста и всех других многомиллионных жертв.

К этому же периоду 1990-х годов относятся и мои неоднократные посещения и работа в Польше. Поскольку я перед этим более-менее изучил польский язык, благодаря автобусу от Тихорецкого проспекта до 9-й линии Васильевского острова, на котором я четыре раза в неделю ездил из моего дома до матмеха ЛГУ, то при первом же удобном случае, а именно, когда заместитель директора польского “Государственного института связи” посещал наш Бонч, а меня пригласили на разговор с ним, как переводчика, я получил от него персональное предложение поработать ПОКА (?) в этом институте месяца четыре, с чем я сразу же и согласился. Приехав в Польшу, я поселился в служебной квартире по соседству со зданием института, который располагался не в самой Варшаве, а в поселке Miedzeszyn, примерно в 40 км от столицы. Моя работа там требовала, правда, моего присутствия целый день в здании института, причем в это время я общался с сотрудниками, проводил для них семинары по различным научным вопросом и, в конце концов, уже после второго посещения этого института в течение двух месяцев в следующем году, написал на польском язы-

ке и издал, монографию по некоторым теоретическим вопросам обеспечения информационной безопасности [7]. В Польше работали два моих хороших знакомых (оба были аспирантами Л.М. Финка в СССР); один из них, Анджей, был настоящим поляком, а вторая – Соня была его женой и приехала на постоянное место жительство из России. Во время моего пребывания в Польше, я часто бывал у них в доме, где, в частности, в их квартире жило 7 котов и кошек (забота о кошках, как своих, так и уличных, была слабостью Сони). Анджей работал доцентом в варшавском Политехе и был хорошим программистом. Поэтому я иногда привлекал его (и не бесплатно, но за счет института) к разработке и демонстрации на моих семинарах различных программ по методам криптографии с открытым ключом. Кроме того, я выступал также по приглашению, причем на польском языке, на межбанковском конгрессе, который проводился один год в Варшаве.

Конечно, будучи в Польше, достаточно долгое время, и прилично владея языком, я попытался познакомиться с польской культурой, природой и местными обычаями. Неоднократно посещал Muzeum Narodowy, где были, прежде всего, достаточно полно представлены картины таких известных польских художников, как Врублевский, Мальчевский, Вычулковский, Матейко и др. Вообще, во время Великой отечественной войны (ВОВ) Варшава была почти полностью сравнена с землей и потом построена заново. Поэтому тут нет значимых исторических памятников. Даже знаменитый Королевский Замок – это “новодел”. Тем не менее, всегда было приятно погулять в знаменитом парке Лаженки, съездить в дворцовые комплексы Виланова, посидеть в уютных варшавских кафе, пройтись по главной улице Nowy Swjat.Тут же вспоминаются известные песенки на польском языке, исполнявшиеся Эдитой Пьехой, Анной Герман и Анной Джантер, безвременно погибшей в авиатеракте над Шотландией, и другими: “Patrze na twoe fotografiju, ktoru dzis przyslal uz me i ty powerzyc ne potrafie…” или “Na francuzskej, na francuzskej est newielka kawiarenka...”. Гулял я по этой улице в Варшаве специально, но похожую kawiarenku, увы, не нашел). На одном из религиозных праздничных шествий, почти рядом со мной прошел тогдашний Президент Польши Lech Walensa, хотя и в толпе, но безо всякой видимой охраны.

Конечно, основные исторические памятники находятся в Кракове, который во время войны совершенно не пострадал. Там сохранился и Королевский замок и средневековые улочки. Именно в Краков на центральную площадь, где тогда собралось около миллиона людей, приезжал и тогдашний Папа Иоанн Павел II.

Я тоже приезжал на эту встречу с группой прихожан из Варшавы. В ожидании прибытия Папы и потом коллективной молитвы, я простоял на этой площади, никуда не отлучаясь, часов 5-6! Помимо этих двух важнейших польских городов Варшавы и Кракова, я побывал в Польше в таких городах как Вроцлав, Гданьск, Ченстохув (в последнем находится знаменитая икона Matka Boska Chenstochowska), и в Познани, причем, не как турист, а, как докладчик на международных конференциях. Так во Вроцлаве, я представлял от Варшавского института связи результаты наших совместных с ним исследований с демон-

страцией эксперимента. Конечно, приличное знание языка значительно расширяло возможности прикосновения к культуре и общение. Так я постоянно смотрел польское TV, специально посещая демонстрацию некоторых польских фильмов, общался с прохожими на улицах.

Приглашали меня остаться и на ПМЖ, продолжая работать в Институте связи; я благодарил, но не соглашался.

В конце своего пребывания в Польше, я на три недели по персональному приглашению профессора Henk van Tilborg съездил в Технический Университет Эндховена (Нидерланды). Результатом этого визита была совместная работа с ним и с A. Barg. (Второй соавтор был из России, но тогда он тоже временно работал в этом университете, а потом уехал со своей женой в США на ПМЖ. Там он работал в одном из университетов и активно участвовал в деятельности общества IEEE on IT.) Работа наша была посвящена решению проблемы распределения широковещательных ключей на основе использования такого аппарата комбинаторики, как неполные сбалансированные блок-схемы (я уже писал раньше, что первоначально, эта идея пришла мне голову, когда я еще учился в ЛГУ). В дальнейшем, эта работа была доложена A. Barg на одной из международных конференций и затем опубликована в книге Lecture Notes in Computer Science [8]. Во время этого визита я также выступал с докладом на семинаре компании Сименс. Пытался предложить кодовое зашумление для реализации, но как-то мое предложение не нашло там позитивного отклика. В один из выходных дней я съездил в Антверпен, чтобы там посетить музей-квартиру Рубенса. Оказался приятно удивлен, что в этом музее нашлось несколько его картин с обнаженными женскими фигурами, причем отнюдь не полнотелыми, как я привык раньше видеть аналогичные его картины в нашем Эрмитаже.

Вернувшись в Польшу, я отработал там эти три недели, чтобы не нарушать моего контракта с Институтом связи.

Хотя я поступал профессором в ЛЭИС на кафедру ТОСиР, но уже в 1990-х годах у нашего ректора Г. возникла идея создания новой кафедры информационной безопасности, тем более, что появился и кандидат на заведование такой кафедрой. Это был президент фирмы “Ланк” В.П.П. (кстати, эта фирма располагалась в том же здании, что и ЛЭИС и ему принадлежащем). Очевидным плюсом такого решения было и то, что от фирмы “Ланк” ожидалась спонсорская помощь. При разговоре с ректором я тоже поддержал, как создание новой кафедры, так и кандидатуру заведующего. Действительно, решение о создании такой кафедры давно назрело, поскольку, с одной стороны, передаваемая и хранимая информация нуждается в такой защите, а, с другой стороны, именно связной учебный институт должен, казалось бы, быть базой для такого изучения. Спустя некоторое время такая кафедра была создана и В.П.П. начал ею заведовать. Предполагалось, что, по крайней мере, два курса “Введение в информационную безопасность” и “Основы криптографии” должны составить базу лекционных курсов на этой кафедре, в связи с чем я занялся подготовкой курса лекций и разработкой программ для лабораторных работ.

Я был очень рад, что благодаря демократизации России, криптография перестала быть “Terra incognita”. Раньше даже слова “криптография”, “шифро-

вание", "ключи" нельзя было писать в открытой литературе и использовать их на лекциях, причем так было только в СССР и сначала в РФ. Считалось, что это дело другого ведомства. Против такого подхода говорило и то, что недавно появились такие открытые стандарты стойкого шифрования как ГОСТ и AES, а также потребность в практическом использовании цифровой подписи, которая основана на криптографии с открытым ключом. Данное решение не исключало, конечно, того факта, что разработка новых криптосистем и строгая проверка их стойкости остается прерогативой этого ведомства. (Как сказано было в Евангелии "Богу – Богово, а кесарю – кесарево.") Не зная даже основ криптографии, наши студенты не смогли бы понять необходимость использования различных узлов в современных стандартах. Кроме того, в криптографии, помимо процедур шифрования/дешифрования важно понимать и некоторые другие ее алгоритмы, такие, например, как аутентификация, цифровая подпись и криптографические протоколы. Симбиоз открытых и закрытых знаний обогащает и последние, не раскрывая закрытости государственных криптосистем. Таких известных мне лично западных ученых, как М. Хеллман, В. Диффи, А. Шамир, Д. Месси. Хенк Ван-Тилборг, Д. Брассард и других нельзя отнести к полностью закрытым криптографам, но именно они внесли существенный вклад в прикладную криптографию, благодаря возможности открыто обсуждать получаемые ими результаты в общедоступной литературе. Имеется немало примеров, когда утаивание результатов работ под грифом, привело как к их тупиковости, так и к утрате приоритета.

Отметим, что созданная в ЛЭИСе кафедра информационной безопасности, была одной из первых кафедр с похожим названием и уж точно первой среди телекоммуникационных университетов.

Долго "засидеться" на одном месте мне не пришлось – вскоре я уехал (а точнее улетел) в Дамаск. Работа в Дамаске оказалась достаточно напряженной: шесть дней в неделю (кроме мусульманского "воскресенья" в пятницу) и по 2-4 часа в каждый из этих дней. Народу на мои лекции собралось достаточно много, не меньше 50 человек из совершенно разных институтов. Жилье мне устроили в довольно комфортабельном коттедже. Возле моего дома постоянно дежурила белая "Волга" с шофером в моем (казалось бы) распоряжении, но, в действительности, я ей смог воспользоваться лишь один только раз – после окончания всех моих лекций, когда меня отвезли на берег Красного Моря для одноразового купания, поскольку в другое время мне приходилось или проводить занятия, или готовить слайды.

По прочтении курса я не получил никакого гонорара и только восточную скатерть в качестве подарка. Правда, перелет, проживание и питание оплачивала принимающая сторона. Пару раз меня приглашали на обед в ресторан организаторы лекций, в который входило и угощение кальяном. Я разрешил также хозяевам пользоваться моим слайдами, написанными на English, и после моего отъезда не знаю делают ли они это сейчас? Но я не был в обиде за такой не очень доходный прием (особенно после приличных профессорских гонораров в Норвегии и Польше) поскольку Сирия не богатая, да еще и воюющая страна. С другой стороны, я получил возможность посетить довольно экзотическую Во-

сточную страну (а Восток меня всегда привлекал) и ознакомиться с ее обычаями и культурой. Конечно, посетил я и самую большую мечеть Дамаска (Омейядов), а каждое утро в 5-6 часов меня будили крики муэдзинов, призывавших правоверных на утреннюю молитву. Правда, теперь муэдзин вещает не своим голосом, а при помощи loudspeaker. Мне сказали, что в Дамаске около 500 мечетей и каждое утро муэдзины кричат из них, призывая верующих мусульман на молитву. Так что после 5-6 часов утра мне уже спать не удавалось Минареты этих мечетей подсвечены зеленым (мусульманским) цветом, что довольно красиво и экзотично.

В конце 1990-х годов у меня состоялись две небольших поездки в Англию. Целью первой было участие в работе научного семинара “Fast Software Encryption”, где я сделал свое небольшое сообщение по кодовому зашумлению. В свободное от докладов время было конечно интересно посетить много мест в знаменитом Кембридже. Жил в частном секторе, хозяйка которого несмотря на зиму, включала обогрев только ночью и поэтому я старался днем туда вообще не приходить. Посетил, конечно, “The blue bar”, в котором часто пивал пиво сам Ньютон, прослушал органный концерт в “King’s Colledge”, прогулялся по знаменитому кембриджскому мосту, который сравнивают с похожим “Мостом Вздохов” в Венеции. Забыл отметить, что так как я попал в Кембридж конечно через Лондон, то и там смог провести пару дней. Посетил британский музей, где меня привлекли картины английских маринистов вполне конкурентные с нашим Айвазовским, посмотрел развод караула у Букингемского дворца, заглянул в Вест-министерское аббатство и посетил могилу Черчилля, которую всем позволено попирать ногами. Перешел даже Темзу по знаменитому из одноименного кино – Мосту Ватерлоо.

После окончания семинара в Кембридже, я поехал на поезде в Ланкастер, где у меня было приглашение от моего старого знакомого, с которым мы встречались на конференциях в СССР, иранца по происхождению, посетить тамошний университет, где он сейчас работал и сделать там небольшое сообщение по концепции подслушивающего канала А. Вайнера. Обратная поездка из Ланкастера в Кембридж ознаменовалась небольшим приключением. Дело в том, что той зимой в Англии были снежные заносы и поезд шел с опозданием на 4 часа, что, конечно, ЧП для Англии. Запомнилась мне эта поездка еще и потому, что в Бирмингеме у нас была, в связи с этой задержкой, почти часовая остановка, и я решил выйти на вокзал. Там, с большим удовольствием купил себе чашку дымящегося шоколада – это было особенно памятно во время такой неожиданной зимы. По приезде на вокзал в Кембридж, нас ожидала дюжина такси для развоза опоздавших пассажиров, а через некоторое время всем опоздавшим заплатили по 150 фунтов стерлингов за доставленные неудобства.

Во время моего другого заезда в Англию, я откликнулся на приглашение из Университета Оксфорда сделать доклад на семинаре в Calderonlab. Тема моего доклада была обозначена так “Протоколы квантовой криптографии”. Дело было в том, что с некоторого времени (по-моему, с одного из семинаров в Дагштуле, где я встретил автора одной из первых статей по квантовой криптографии J. Brassard), я заинтересовался этим научным направлением. Действитель-

но, используя квантовую криптографию (не путать с квантовыми компьютерами – это совсем другое!) можно обнаруживать вторжение в квантовый канал и, следовательно, безопасно передавать ключевые данные тогда, когда такого вторжения не было. Почти сразу же, я пригласил J/Brassard-a прочитать лекцию в Бонче, что он вскоре и сделал, а моя дочка еще и выступила для него гидом по Петербургу. Тему по квантовой криптографии я выбрал и для одного из моих способных аспирантов К. Так что, к моменту моего посещения Оксфорда, у нас накопился уже некоторый научный материал по этому направлению. По договоренности с тогдашним нашим ректором, даже предполагалась и заказная НИР с одним из физических институтов в Москве, но, вдруг, все рухнуло. Во-первых, внезапно умер ректор, который это направление активно продвигал, во-вторых, главный предполагаемый исполнитель этой НИР уехала работать за границу, наконец, в-третьих, я понял, что слишком стар (точнее недостаточно молод) для такого направления исследований. Конечно, мы могли бы разработать протоколы и первоначально оценить их эффективность, но надо было исключить возможность проведения перехватчиком любых изощренных (точнее translucent) атак. А это уже требовало не только понимания математических формул квантовой физики, но и глубокого понимания физического смысла различных квантовых преобразований, и я решил, что уже не в состоянии их понять или, точнее говоря, вообразить их себе (вспоминается анекдот про Чапаева и квадратный трехчлен…). Так что для меня это направление в высоком смысле закрылось, почти и не начавшись, хотя мой аспирант К. успешно защитил кандидатскую диссертацию и затем стал доцентом нашей кафедры, но никаких фундаментальных достижений, включая и практическую реализацию, мы в будущем, увы, не сделали. Ну а вот прыткие китайцы, насколько я помню, даже построили протяженную оптико-волоконную линию связи с квантовой криптографией. Впрочем, как это типично для них, они, наверное, не заморачивались со всякими там полупрозрачными атаками.

Возвращаясь к моему посещению Оксфорда, сделаю еще некоторые бытовые зарисовки. Поселили меня в гостинице для приезжающих ученых, и, действительно, какие только звезды мировой физики там на бывали! Еще меня поразили мраморные доски, где были перечислены имена всех ректоров Оксфордского университета, начиная с … 14-го века! (Боюсь, что у нас в университетах даже не всех великих князей и царей знают с того времени.) В качестве местной экскурсии я посетил университетскую библиотеку, где наряду с современными книгами, хранились тяжеловесные фолианты 13-14 веков. Члены общества, окончивших Оксфорд, имели персональные (аршинные по размерам) ключи от этой библиотеки и могли ее посещать в любое рабочее время и безо всякого контроля. Последнему я особенно удивился и даже (позорно) спросил: “А если кто-то какую-нибудь древность стибрит?” На меня довольно презрительно посмотрели и ответили, что тогда его из этого общества исключат, хотя такого пока еще не случалось и не должно случиться. После моего доклада отвели меня в профессорское отделение столовой. Но что это была за столовая! В полумраке повар в белоснежном колпаке предлагал вам на выбор кусищи тушеного мяса. А десерты в виде пудингов, тортов и др. были выше всех похвал! В доба-

вок, все это продавали довольно дешево (со специальной скидкой для студентов и преподавателей) – вот почему, наверное, у них так много Нобелевских лауреатов… Наконец, почти как Остап Бендер, попавший под лошадь, я чуть было не попал, правда, под Ostin, когда, переходя улицу, сначала поглядев налево – у англичан многое не как у нас – правостороннее движение, например.

В 1998 г. состоялась моя первая поездка в США в г. Charlotte (North Caroline), куда я был приглашен для чтения пятинедельного курса лекций “Основы криптографии”, вставленного в расписание Summer courses, и за посещение которого каждый студент должен был заплатить несколько сотен долларов. Отмечу еще раз, что, как и во всех других случаях моих заграничных лекций, я получил приглашения в USA не через администрацию Бонча, а по личной договоренности с одним профессором этого университета (поляком по национальности), с которым я встретился во время моей работы в Польше. Но администрация Бонча разрешила мне краткосрочный отпуск для такой поездки, правда, безо всякого финансирования. Она понимала, что, во-первых, я там смогу немного подзаработать, во-вторых, приобрету дополнительный опыт преподавания иностранным студентам на English, который мне может пригодиться и в Бонче и, наконец, в-третьих, делаю promotion нашему университету. Я был благодарен ей за это понимание. Конечно, я чувствовал большую ответственность при подготовке к этим лекциям, поскольку понимал, что USA это страна, где работают профессора разбирающиеся (не совсем адекватное слово…) в криптографии. К моему счастью, таких людей не нашлось сейчас именно в этом университете, а желающих послушать меня набралось достаточно много – два потока человек по 50 в каждом, причем по возрасту тут были не только студенты, но и 40-50 летние слушатели. За основу этого курса я взял наш аналогичный курс в Бонче, подготовленный на таких зарубежных источниках как [9, 10]. Кроме того, я подготовил около десятка компьютерных программ для проведения занятий, поясняющих работу криптоалгоритмов и в конце курса надо было еще мне принять экзамены у каждого студента и проставить им оценки. В целом, все прошло более-менее спокойно, хотя некоторые студенты были не очень довольны моими невысокими оценками и даже жаловались на это декану. Одна из студенток попросила меня принять у нее экзамен заранее, так как она куда-то уезжала. Я согласился, но попросил ее не разглашать вопросы билетов другим студентам. Она очень удивилась моей просьбе и сказала: “как же я им открою содержание вопросов в билетах, ведь тогда они смогут сдать экзамен лучше меня?” Ответ этот меня удивил – у нас в стране было бы не так… Как-то я зашел в университетскую библиотеку посмотреть, нет ли там дополнительных книг по криптографии? Библиотекарь ответил мне, что, вроде, тут подобные лекции читает какой-то русский – может мне у него спросить? Он был очень удивлен, узнав, что я и есть тот самый русский. Состав слушателей моих лекций был довольно разнообразный по национальностям – часть природные американцы, часть – темнокожие и довольно много китайцев. Как-то гуляя по окрестностям, я познакомился с одной слушательницей моих лекций – китаянкой и узнал от нее много интересного о жизни в Китае. (Кстати, несмотря на несколько приглашений, я никогда не хотел почитать лекции в Китае. Конечно,

современный Китай это ого-го по виду, но мне казалось, что дух “мандаринов и битья по пяткам” там все же еще сохранился.

Мне предоставили в качестве рабочего места отдельную комнату с персональным компьютером, как и положено здесь любому Full Professor, хотя бы и временно работающему. Поскольку я читал лекции в июле, то жара тогда была страшная, несмотря на North, а не South, Caroline… Однако, я сидел в своей комнате даже в довольно теплой куртке, поскольку у меня там стоял кондиционер, который никак не могли отрегулировать – вот тебе и USA! По местному радио даже объявляли, что в эти жаркие дни пожилым людям не рекомендуется даже выходить на улицу... (Мог ли я себя отнести к пожилым в 62 года – ну раз уж назвался груздем, то и полезай в этот американский кузов…) Жил я на кампусе в небольшом одноэтажном домике, конечно, со всеми удобствами и в двух шагах от университета. Обедал в университетской столовой (вполне терпимой). А завтракал и ужинал у себя дома. Однако, на кампусе никаких магазинов не было, и ближайший из них находился километрах в пяти, причем идти туда надо было по тропке вдоль оживленной автострады. По воскресеньям я так и делал. Таким же путем перемещались только... (чуть не сказал негры, конечно же afroamerican). Белые же люди катили мимо на шикарных машинах. Я, конечно, мог бы купить и себе какую-нибудь подержанную машинку на аванс за лекции, но решил перенести небольшие унижения и этого не делать. Куда же я ее через месяц дену, в конце концов? Ближе я познакомился с одним из моих студентов-американцем. Основной темой наших бесед в перерывах и после лекций были местные торнадо – жуткое дело! В один из выходных дней я съездил в Вашингтон на автобусе. Посмотрел на Капитолий, Белый дом, сенат и на всякие монументы. Посетил музей жен первых леди Америки. Понравился мне железнодорожный вокзал, но не метро – там страшновато. Хотел попасть на Арлингтонское мемориальное кладбище (в качестве визитера, конечно), но что-то там не срослось. Приехал я на метро. Поднялся на эскалаторе и вдруг он вынес меня прямо к дверям (вы не поверите!) … Пентагона. Я быстренько развернулся и поехал вниз. Так вот он какой, этот “Страшный Бармалей” – которым нас много лет пугали... Как-то в выходные я примкнул к группе туристов, которые ходили по отрогам Аппалачей. Виды были довольно симпатичные, но что меня там поразило, так это множество одиночных туристов, которые шли не глядя по сторонам на природу – главное им надо было уложиться в какое-то там время и … следовать указателям.

Еще один случай произошел у меня в Шарлоте во время грозы в выходной день, когда я сидел в своем рабочем кабинете. Вдруг, после сильного удара грома сработала противопожарная сигнализация. Я осмотрелся, потянул носом воздух –ничего вроде не горело, а сигнализация продолжала звенеть. Позвонил своему профессору и он мне посоветовал связаться с … полицией, что я быстро и сделал. Полицейские посоветовали мне закрыть кабинет и покинуть здание, а на улице лил сильный дождь. В итоге я промочил несколько своих дисков для компьютера. Вот так я провел ТЕМ летом в USA.

5. Жизнь и работа в Мексике

Моей долговременной поездке в Мексику предшествовала кратковременная (пробная) поездка, включавшая встречу с руководством CINVESTAV. Это университет, в котором предполагалась моя работа в дальнейшем. (Для краткости я буду этот университет называть далее “Cin”). Проба прошла благополучно и зам. ректора (по-нашему проректор) сказал мне, что я смогу поработать в Cin столько, сколько захочу – ха-ха – это оказалось совсем не так!

И вот, наконец, после многомесячного ожидания приглашающих меня документов (в частности специальной формы FM-3), я с двумя большими чемоданами выхожу в зал ожидания, где меня встречает мой конфидент, приехавший много раньше, в Cin, но тоже из нашего же Бонча и работающий здесь уже 3-5 лет профессор К. Садимся на его шевроле и едем по городу, в уже известный мне универ, а точнее, в съемную квартиру тоже одного русского доцента из Физтеха в Питере, который уже работает в Cin и предполагается, что я поживу некоторое время в его квартире, пока не сниму свою. Проезжаем по Avenida Politechnika мимо нескольких небольших банков, где я почти везде замечаю стоящие с мигалками полицейские машины. К. поясняет, что это, мол, обычное явление – была попытка ограбления – народ то тут, в основном бедный, надо же как-то подзаработать... Приезжаем в мое временное жилье. Вхожу в комнату, ставлю на пол свои чемоданы и чувствую некоторое волнение – ведь я приехал сюда не на неделю, и даже не на месяц, и не как турист, а как работающий человек, которому предстоит далее самостоятельно заниматься и своим бытом. Не отвергнет ли меня эта цивилизованная, но пока мне совершенно неизвестная среда? Все, однако, произошло довольно дружественно. Я быстро познакомился с русскими профессорами, работающими в Cin, а их было не мене 10 человек. Быстро узнал свое расписание занятий на этот год. Причем их было не более 4-6 часов в неделю, включая лекции и лабораторные занятия, но с обязательной выдачей домашних заданий в виде “home work” каждую неделю и экзаменов в конце каждого семестра. В группе оказалось 20-25 человек уже имеющих дипломы бакалавров от других университетов. Уровень знаний студентов, пожалуй, был пониже, чем у нас, но усердия больше и посещаемость выше. Технические средства обучения – это слайд-проектор для слайдов, которые у меня не были заранее подготовлены и поэтому нужно было их здесь рисовать и представлять на лекциях “прямо с колес”. При проведении групповых занятий и лабораторных работ, использовались персональные компьютеры студентов (один на двух человек), а каждому преподавателю предоставлялся, конечно, свой персональный компьютер. Курс “Теория электрической связи” (ТЭС), который мне предстояло здесь читать, был хорошо известен мне по Бончу, но тут мне, конечно, предстояло перевести его на “English”. Более того, я мог дать им более глубоко те разделы, которыми сам занимался в плане научных исследований. Это, прежде всего, теория информации, включая и теорию помехоустойчивого кодирования. Правда, к каждой лекции мне приходилось дома рисовать на “English” по 10-15 слайдов формата А4 цветными фломастерами, что конечно требовало определенного напряжения и самодисциплины.

В течение первого года все шло спокойно. Параллельно я занимался исследовательской работой, которая в моем случае, заключалась в написании статей в международные журналы и подготовкой докладов на международные конференции. (Интересно отметить, что как бы это не выглядело непатриотичным, но местные (то есть мексиканские) издания тут не принимались во внимание и в зачет шли только публикации в США, Европе или в Азии (Японии). Направления моих публикаций оставались прежними, то есть бесключевая криптография, включая распределение ключевых данных по каналам связи. Именно по это теме я сделал доклад по приглашению на международной конференции в Орландо (США), а также на ежегодном семинаре “Serias security seminar” в университете Purdue штата West Laffaet (USA). Воспользовавшись тем обстоятельством, что в универ Purdue я добирался через Чикаго, я посетил знаменитый чикагский художественный музей и поднялся на последний этаж небоскреба Emperial State Building, который ранее считался самым высоким зданием мира, но теперь конечно уступает по высоте многим другим небоскребам, особенно в Эмиратах

Наиболее значимой моей работой в этот период времени был мой доклад на международной конференции по “Information Security” в Испании. Он был посвящен формулировке и доказательству теоремы усиления секретности, которая ранее, но в менее общей форме, была доказана U. Maurer. Эта работа была потом опубликована в издании [11]. Еще один важный доклад был подготовлен и потом сделан на международной конференции IEEE on IT в г. Сорренто (Италия) совместно с моим аспирантом Б., который потом покинул меня, так и не завершив свою диссертацию. Сорренто симпатичный городок на берегу Средиземного моря, но конференция проходила в его центре, где до моря оказалось довольно далеко. Поэтому я каждое утро перед заседаниями спускался к морю по крутой лестнице и с полчаса плавал там в уютной бухточке, вспоминая песню “Вернись в Сорренто, тебя я жду.” Сплавал на катере на знаменитый остров Капри, где некоторое время жил М. Горький. Надо признать, что “Буревестник революции” выбрал для совместного отдыха с актрисой Андреевой неплохое местечко… Правда, сейчас к острову все время прибывают катера и туристы тысячами валят по узким улицам наверх, наверх. Туда можно подняться и на фуникулере, что я и сделал, и обнаружил наверху в кафе, сидящего там с женой известного ученого из Японии Тадео Касами. (Мы про него шутили с коллегами из России – “Касами, но с волосами”). Я, будучи знакомым с ним по другим конференциям, присел к ним за столик и выпил чашечку кофе. Чудесный вид открывался с вершины острова на крутой, наверное, двухсотметровый обрыв и море под ним.

Чтобы закончить описание моей исследовательской работы в Мексике и перейти к тому, как люди живут и работают в Мексике и какова природа этой горной и одновременно тропической страны, скажу немного о некотором новом тренде моих исследований в конце моего пребывания в этой стране. Действительно, я начал там заниматься совершенно новым для меня направлением “Стеганографией” и “Цифровыми водяными знаками”, хотя в мировой научно-технической литературе это направление развивалось уже не менее 5-7 лет под

общим названием “Information Hiding”. Когда я увидел в статьях этот термин, то даже не мог сначала предположить, к чему он относится? Оказалось, что, вообще говоря, эта область науки весьма занимательна и достойна своего развития. Буквальный перевод на русский язык слова “стеганография” означает “утаивание информации”. (Не надо его путать с общеизвестным словом “стенография”, что буквально переводится как “узкое письмо”, а реально оно используется для быстрой письменной фиксации устной речи. (Тут сразу вспоминается стенографистка Ф. Достоевского, которая со временем стала и его женой). Стеганография же означает совершенно иное – это такое преобразование различных объектов, содержащих основную информацию (неподвижные изображения, видео, печатный текст, звук и даже другие более экзотические носители, например, коды источника или описания химических элементов формулами), в другой аналогичный объект, который, сохраняя высокое качество основной информации, позволяет легитимным пользователям извлекать из этого преобразованного объекта некоторую новую информации, которая оказывается недоступной для нелегитимных пользователей. Таким образом, в отличии от криптографии, где главная задача состоит в закрытии содержания сообщений, в стеганографии основная задача заключается в том, чтобы утаить и сам факт присутствия этого дополнительного сообщения в данном покрывающем объекте. В некоторых публикациях такой покрывающий объект назывался “контейнером”. Мне такой термин не кажется удачным, поскольку контейнер всегда предназначен для какого-то погружения в него, а наблюдаемый контейнер в стеганографии может быть часто и ничего не содержащим. Казалось бы, стеганография (СГ) должна применяться, прежде всего, в каких-то государственных структурах, но в последнее время она появляется и в бизнес-сообществе, причем, в основном для решения задачи обнаружения СГ, например, как в известной системе DLP с целью пресечения промышленного шпионажа.

Цифровые водяные знаки (ЦВЗ) выполняются похожими алгоритмами вложения, но цель у них несколько иная – обеспечить невозможность удаления вложенных ЦВЗ без значительного искажения покрывающих объектов. Причем задача скрытия присутствия вложения для ЦВЗ не обязательна. Очевидно, что основным практическим применением ЦВЗ должно быть обеспечение прав собственности (copyright) для различных мультимедийных объектов. Некоторое охлаждение к криптографии в пользу СГ и ЦВЗ объяснялось у меня тем, что основная задача криптографии представляется слишком “глобальной” – взлом стойкого шифра или разработка такого стойкого шифра, который невозможно взломать в обозримое время или при обозримом объеме оборудования. Решение этих задач для современных шифров требует специального образования и приводит к требованию значительных вычислительных ресурсов. Так, как повезло английской группе ученых, работавших в Blatchly Park с участием A. Turing и взломавшей стойкий на то время немецкий шифр “Энигма”, вряд ли повезет какой-то группе сейчас при взломе стойкого шифра вроде 3DES или AES, даже если они будут вооружены сверхмощными компьютерами. Другое дело СГ, когда вполне реально построить почти необнаруживаемую СГ или ЦВЗ, защищенную от удаления для целого комплекса атак. Интересно еще и то, что реше-

ние этих задач требует математического аппарата близкого в матаппарату теории электрической теории связи. Это статистика, теория кодирования и теория информации, которые и ранее были мне достаточно близки. В конце моего мексиканского периода мне удалось опубликовать (в соавторстве) несколько работ, связанных с построением систем ЦВЗ, например [12]. Этой тематике были посвящены и два мои доклада в Канаде (Kingstone and Vancouver). Скажу пару слов об этих поездках. В Kingstone я ехал по Великим американским озерам на корабле через канадский город Торонто. Этот город ничем особенным не знаменит, кроме того, что совсем недалеко от него находится Ниагарский водопад. Это чудо природы, конечно, замечательно, но особенно поразило меня то, что прямо из улицы, вдруг, только повернув, попадаешь на набережную реки, на которой и находится этот самый водопад, уж очень это как-то по-домашнему… Что же касается Vancouver-a, то город этот очень живописен. Только лишь заселившись в отель, я подумал, что ни на какую конференцию не пойду, а буду сидеть в номере и из окна любоваться на корабли, подплывающие к живописной бухте и смотреть на окрестные горы (холмы), а потом – ездить туда на фуникулере. Но, конечно, это была шутка и мне очень запомнился доклад канадского председателя общества IEEE, который показал, что результат почти каждой значительной теоретической статьи, помещенной в журнале IEEE on IT, был через некоторое время реализован практически или в мобильной или в спутниковой связи.

Ванкувер еще знаменит своими городскими часами, которые от всех других подобных часов отличаются тем, что работают на “паре” и издают временами резкие гудки похожие на паровозные. После окончания конференции в Ванкувере, мы с моим знакомым канадским профессором S. поехали на автомобиле, управлявшемся бывшей аспиранткой из России, на многодневную экскурсию по острову Viktoria, где меня особенно удивили деревья-гиганты и объявление на морском пляже о наличии в море “rip current”, то есть мощного течения, которое может тебя при купании унести в открытый океан, и тогда все...

Теперь я перехожу к описанию условий моей работы, а также особенностей природы и жизни мексиканцев. Замечу сначала, что когда я говорил своим знакомым, что собираюсь поработать в Мексике, то многие мне сочувствовали – мол там очень жарко. Однако, это оказалось мифом. На самом деле Мексика это, в основном, горная страна, в частности столица ее Мехико находится на высоте 2200 м над уровнем моря. Поэтому летом там не бывает очень жарко, максимум 25-30 градусов, а зимой может быть иногда даже весьма прохладно и может выпасть небольшой слой снега с утра, который, обычно, днем тает. Конечно, когда спускаешься с нагорья к Тихому Океану, который тут все называют Pacific, то в этой области царят тропики с их жарой, влажностью и с запахом различных тропических растений. (Об этом я напишу более подробно, когда дойдет рассказ до отдыха на океане). Вообще-то климат в Мексике муссонный. То есть полгода с сентября до марта – солнце, а с апреля до августа – дождь. (Но, конечно, не такой непрерывный дождь, который описан в одноименном рассказе С. Моэма, то есть непрерывный ливень, когда все с ума сходят.) Просто бывают сильные и даже продолжительные дожди в летний период и уж

точно не одного дождя – в зимний период. Как я уже упоминал раньше, Мексика, в основном, горная страна. Горы, как правило, покрыты хвойным лесом (соснами с длинными иглами и с огромными шишками). Высоко в горах растительности уже почти нет и лежит только снег и лед. Наиболее высокие горы это известный Попокатепетль и менее известная Аризаба, высота которых превышает 5000 м. Вершины, по большей части, представляют собой вулканы, причем действующие, которые постоянно курятся, а иногда и извергаются. На дорогах близких к таким вулканам стоят таблички с надписью “Ruta de evacuacion”, то есть “маршрут эвакуации”, а то, при неверном маршруте, засыплет пеплом, как бедолаг в Помпее.

Теперь кратко о населении... Конечно в Мексике живут мексиканцы, но не только они, но еще есть и испанцы, индейцы и много других национальностей. Удивительно, что в стране почти не живут негры, то есть чернокожие (прошу прощения, что я не употребляю это длинное слово афроамериканцы). Причина этого, прежде всего, в том, что завоз рабов на плантации был здесь не рентабелен, так как тут нет больших посадок хлопка или маиса (кукурузы), а кофе, конечно же, растет, но не так массово и не так удобно, чтобы его можно было бы выгодно широко разводить. Есть и другая версия того, что латиносы просто не уживаются с неграми, которая, наверное, и не лишена смысла, но в Бразилии полно последних, хотя это страна латиносов, причем португальскоговорящая. В столице живет около 20 миллионов людей, правда, я думаю, что большинство из них ютятся в фавелах – то есть в почти в бумажных домиках на окраине города. (Хотя так было 20 лет назад-может сейчас все они переехали во дворцы у моря – шутка). Народ, большей частью, дружелюбный – всегда покажет дорогу и улыбнется Вам. Правда, преступность тогда была весьма высока. Мой конфидент К., как я уже упоминал, объяснял это тем, что народ в большинстве своем бедный и ему как-то надо подзаработать. Во время моего пребывания в Мексике случалось немало случаев бандитизма, правда, не со мной, но с моими близкими знакомыми. Иногда войдет такой бедняк в микро автобус, достанет кольт из кармана (“Макаров” тут редок) и отберет у всех пассажиров – телефоны, кошельки и украшения. Другое типичное ограбление – это постучать тем же кольтом в стекло автомобиля, стоящего на перекрестке перед красным светом светофора, и горе тому водителю, который попытается газануть и уехать, хотя мне встречались, по их рассказам, и такие. Одного моего коллегу, тоже из Питера подловили в центре города (возле главного собора на площади Zocalo) на улице где продают сувениры, слегка придушили, обшарили карманы и потом отпустили, а толпы народа вокруг никак на это не реагировали. Вообще, существует здесь такое мнение, что все gringos (то есть – чужие) богатые и носят много денег при себе. Этот русский профессор потом долго кашлял из-за боли в придушенном горле. Особый разговор о местной транспортной полиции. Наша, по сравнению с ней, это идеал заботливого отношения к гражданам! Мы, когда проезжали на машине одно место, знали, что там всегда стоят полицейские и отлавливают водителей-иностранцев. Причем всегда найдут к чему придраться – или пассажиры сзади не привязаны, или ты не показал знак поворота, хотя ты его точно показал и т.п. Подходят, забирают документы и говорят, что-

бы пришел за ними в полицию, скажем, через месяц. Конечно же, вымогают штраф и немалый. А что так много спрашиваю – а ты видишь, вон еще там вдалеке стоит другой ловец-полицейский – ему ведь тоже надо от нас дать? Вопиющий случай рассказал мне один русский, который уже лет 20 живет и работает в Мехико. Как-то он решил снять деньги с уличного банкомата. Его вежливо пропустил в дверь какой-то мексиканец, но потом юркнул за ним, врезал ему куда-то и потребовал снять с карты максимум, то есть столько, сколько можно. Тот не сопротивлялся, ожидая, что у грабителя в кармане лежит упоминавшийся уже кольт. Потом грабитель убрался восвояси, еще врезав ему напоследок. Каково же было удивление моего знакомого, когда на следующий день он увидел своего грабителя ... спокойно торгующего с лотка на соседней улице. Обратился в полицию и его (не грабителя!) задержали и обвинили в оговоре. Просидев в кутузке несколько часов, он откупился тремястами песо и вышел на свободу, проклиная свою глупость. … Нам рассказывали, что есть такие шоссе, вблизи Pacific, где ночью могут спокойно остановить и забрать машину, а при сопротивлении – просто пристрелить пассажиров. Но мы старались, конечно, не нарываться и ночью вообще по захолустью не ездить. Рассказывали также (и этому можно поверить), что будто, один наш соотечественник-артист гастролировал в Мехико и как-то вечером вышел на центральную улицу Reforma из своего шикарного отеля прогуляться. И вдруг, у него в спину уперлось что-то твердое. Он обернулся и увидел тот же кольт и маленького человечка индейского вида, который знаками показал ему чтобы он достал прямо сейчас свой кошелек. – Да я тебя сейчас – успел только вымолвить наш великан – и тут же получил пулю в колено. Говорили, что потом его вывозили на сцену на каталке…

Вообще, когда я приехал в Мексику, то меня предупредили, что надо соблюдать определенные меры безопасности. Во-первых, я жил в так называемом unidad – это группа домов, окруженная высокой каменной стеной со входом и въездом на территорию по специальным пропускам. Кроме того, сказали, что гулять в Мехико даже в центре в темное время суток небезопасно. Вот этих простых правил мы и придерживались и нам повезло – ни разу мы не столкнулись с преступностью лицом к лицу. А вот у меня была пара знакомых женщин (одна мексиканка, а другая певица местного ресторана, приехавшая из России), так у первой убили парня, а у второй – мужа-мексиканца. Вот такие дела. Однако, Мексика тогда была еще не на первом месте по преступности. Когда один из местных преподавателей Cin уезжал к своим родственникам в Колумбию, то мы провожали его, как в зону ведения боевых действий.

Существуем миф, что все мексиканцы хотели бы эмигрировать в США. Однако, это относится только к беднейшей части населения страны. Что же касается государственных служащих, инженеров различных компаний и преподавателей государственных или частных университетов, то их вполне устраивает работа и жизнь в Мексике. Хотя зарплата профессоров в Мексике несколько меньше, чем в США, но и жизнь там не столь дорогая, как в штатах – в Мексике дешевле снять жилье, купить продукты, взять такси, проживать в отелях и на некоторых курортах даже Тихоокеанского побережья и т.д. Более того, довольно распространенная ситуация, когда американцы, выйдя на пенсию, поселяют-

ся в привлекательных по природе местах Мексики. Типичными являются отгороженные стенами поселения таких пенсионеров со своими магазинами, полями для гольфа, кортами и т.п. Разве плохо на деньги, “заработанные непосильным трудом в США”, отдыхать в местах вечной весны, да еще и при изобилии всяческих тропических фруктов. Появился даже специфический вид занятий для таких “бедных американцев” – “bird watching” – то есть часами пялиться и фотографировать местных птичек в местах их естественного обитания.

Медицина в Мексике также многое заимствовала из США. Правда, лечат там по стандартам, и “чтобы поцеловать” не остается времени

Университеты в Мексике тоже во многом копируют американские. Так Cin, в котором я работал, скопирован с американского Принстона, правда, думаю, что там нобелевских лауреатов, даже в копии, пока еще нет. В Мехико есть зато гигантский Политех, в котором учится порядка ста тысяч студентов, причем, преподают там, наверное, несколько десятков профессоров из России по различным специальностям и совершенно различного научного уровня. К сожалению, есть в Мексике довольно общее и особенно неприятное для меня правило – профессор должен присутствовать на своем рабочем месте (включая конечно и аудитории для занятий) в течение всего рабочего дня. Исключения допускаются только для дальних или ближних командировок, а также при посещении библиотек, предприятий или врачей. Правда, для профессоров созданы для “отсидки” довольно сносные условия – либо комнаты на два человека, либо полупрозрачные клетушки 2×2 метра. Тем не менее, для меня такое ограничение на необходимое присутствие очень мешало научной работе и особенно “размышлениям над листом бумаги”, что я привык делать обычно в домашней обстановке.

С другой стороны, есть в ВУЗах Мексики и вполне разумные, на мой взгляд, правила. Так обучение в университетах бесплатное, но если студент отчисляется по неуспеваемости, то потом, спустя некоторое время, он снова может быть зачислен на тот же курс, но уже на платной основе. Я пробовал предлагать подобное правило и в нашем ВУЗе, но что-то тут не понравилось…

Пара слов об оплате преподавателей в Cin. Помимо базовой (сравнительно небольшой) зарплаты каждому из преподавателю на 2 года назначается свой исследовательский уровень “бека” (nivel, beca) по результатам его научных исследований за предыдущие два года, причем, эта добавка может быть весьма существенной и достигать даже целой базовой зарплаты. Она назначается специальной внешней комиссией (из мексиканской академии наук- Conacyt) по результатам твоей публикационной деятельности, то есть по количеству и качеству печатных работ, причем только в международных журналах. Мне, например, сразу назначили уровень 5б, что, практически, удваивало мою зарплату.

После двух лет работы я должен был отвести в Conacyt оттиски своих работ, индексацию их цитирований и др. общим весом килограммов пять. Однако, это лично мне не совсем помогло, хотя “беку” мне и сохранили, но сочли, что у меня было недостаточно публикаций в научных журналах, а, в основном, они были в трудах международных конференций (причем пусть даже и в таких престижных как SANS, IEEE on IT и т.п.). Поэтому мне дали понять, что на

третий год мой контракт не продлят, несмотря на предварительные заверения замдиректора – “работайте, сколько хотите” и даже с учетом того, что на втором году моей работы я читал курс телетрафика, от чтения которого отказались все преподаватели, а я должен был его взять, хотя в России никогда не занимался данным направлением.

К счастью, подвернулась вакансия профессора в филиале Cin, в городе Гвадалахара (втором по величине городе Мексики). О жизни и работе в этом городе я напишу чуть позже. По приезде в Бонч, я предлагал и у нас завести такой порядок оплаты преподавателей. То есть установить эти уровни и если за пару лет преподаватель ничего не наработал – то и “иди лесом”. Но ректорат с возмущением отверг мои предложения. Сказали, “а как же быть тогда с теми, кто за это время написал только методические работы?” (Прямо как в той народной мудрости: Кто умеет – делает, кто не умеет делать – учит как надо делать, а кто и учить не умеет, тот учит, как надо учить; это и называется – “методист”…)

Замечу еще, что в университете Cin группы студентов были небольшими по 20-30 человек, причем, на нашем факультете телекоммуникации обучалось всего три таких группы. За дипломников шла конкурентная борьба между преподавателями, и не всегда объективная. Так ко мне хотели прийти пять человек, но начальство не разрешило и направило их к “нелюбимому” преподавателю. Один из дипломников, все же, у меня остался и после он поехал в Бонч на полгода, чтобы там свой диплом дописать. Потом я специально был снова на месяц приглашен в Cin, чтобы присутствовать на его защите. (Работу он писал по криптопротоколу тайного голосования). С аспирантами ситуация оказалась еще более сложной. Здесь принято, что у каждого преподавателя может числится не более 2-х человек и мне, конечно, никого не дали. Есть и еще одна позиция это auxilar, что-то вроде ординатуры в медицине. Типично студент на этой позиции помогает своему руководителю и готовится к поступлению на разработку Ph.D. Я думаю, что для руководителя это очень хорошая подмога, поскольку и ему помогают, и проверить способности студента можно лучше, чем при обучении в магистратуре. Приятной особенностью для преподавателей, занимающихся научной работой, является оплата университетом научных заграничных конференций. Если доклад там принят, то можно получить не менее 1000 USD, и даже много больше, если у тебя есть еще НИР от какой-то компании. Принято также платить подъемные, когда поступаешь на работу и каждый год 13-ю зарплату. Я, кстати, на эти подъемные плюс зарплата смог купить себе почти новый автомобиль Chevy (с 3000 км пробега) уже после трех месяцев работы, на котором мы успешно проездили с моей женой Мариной (М) до конца моего пребывания в стране. Однако, самое большое впечатления на меня произвело правило получения subbatical, то есть годового (!) оплачиваемого отпуска, после каждых пяти лет работы. Увы, у меня такого не было и, наверное, никогда уже не будет в России. Во время этого отпуска ты можешь валяться на песочке возле Тихого Океана, получая каждый месяц профессорскую зарплату, или устроиться по контракту на какую-либо другую хорошо оплачиваемую работу (например, в один из университетов USA) с полным сохранением своей основ-

ной зарплаты и с возможностью гарантированно вернуться на прежнюю позицию. Ну разве это не сказка, которая и не снилась профессорам из РФ?!

Итак, мне удалось перевестись в филиал Cin в г. Гвадалахара, который находится примерно в 300 км к северу от Мехико на высоте около 1500 м над уровнем моря, но, все еще, в тропиках. Поэтому там значительно теплее зимой, но зато он и более муссонный, то есть там резче выделяются дождливый и сухой периоды года и дожди сильнее, чем в Мехико, так что иногда улицу переходишь по щиколотку в воде. Зато это город почти "вечной весны", хотя основную пальму первенства в этом вопросе имеет город Carnavaca (в буквальном переводе – коровье мясо, т.е. кратко – "говядина").

Итак, вторая половина моего пребывания в Мексике проходила в городе Гвадалахара. Там я заранее тоже снял квартиру, правда, немного подальше от работы, чем в Мехико. Поэтому мне приходилось ездить туда и обратно на своей машине. На работе мне выделили место в одной комнате с местным профессором, а точнее с Ph.D-стом. (Замечу, что профессором в Мексике иногда называют и дрессировщика на собачьей площадке). Оказалось, что этот кадр очень любил общение и поэтому к нему ежеминутно приходили друзья с нашего факультета и громко болтали, хотя и на испанском, но поскольку я тогда именно этот язык и изучал, то меня это сильно отвлекало. (Правда, немного погодя мне предоставили отдельный кабинет для работы). Остальные условия были такие же как в Мехико. Читал я тот же курс, в группе было столько же студентов, писал статьи и доклады по тем же направлениям. Так прошло полтора года и потом мой контракт не продлили, хотя я особенно на этом и не настаивал. Причина этого "непродления" мне до сих пор не очень ясна, но, думаю, что она никак не была связана с моей работой и отношениями в коллективе.

Теперь не о работе… Особое место среди крепких напитков в Мексике занимает, безусловно, текила. Это, как-бы, мексиканская водка. У нас бытует миф, что она делается из … кактуса. Мексиканцы обижаются на это и говорят – да не из кактуса, а из "agava azul"! Конечно, на первый взгляд, это растение похоже на кактус. Огромные (1,5 – 3 м длиной) толстые листья, которые растут, вроде бы, прямо из земли, а на самом деле, из "шишки", сидящей в земле. Именно из такой "шишки", а не из листьев, и делают текилу. Мы были в посёлке "Текила" – это "бренд" и только здесь делается аутентичная текила, подобно коньяку или шампанскому во Франции. Осмотрели всё производство – как "шишки" очищают (каждая по 25-30 кг весом), ферментируют, делают прозрачный спирт (tekila blanca), потом выдерживают его в дубовых бочках и, напиток приобретает желтоватый цвет. Есть множество сортов текилы и по разной цене, в том числе даже и коньяк из текилы (conecho). При подъезде к посёлку вдоль шоссе стоят, вытянувшись цепочкой, продавцы "самопальной", или может быть, "самокраденной" текилы, которая, конечно, значительно дешевле аутентичной, но и, возможно, опасней для здоровья.

Пара слов о известном музее Л.Д. Троцкого, находящемся в фешенебельном районе Мехико Кайоакане, кстати, все в этом музее оставлено так, как это было в 1940 г., когда, некто Меркадер, проникший, как приятель секретарши Л.Д.Троцкого в его дом, рубанул голову бывшего "льва пролетарской революю-

ции”, вытащенным из портфеля ледорубом (вот что значит – не было тогда металлоискателей!). От этого удара Лео Троцкий скончался через день или два в госпитале. Меркадера повязала охрана Троцкого, его судили, приговорили к 20-ти годам тюрьмы, где он и отсидел свой срок “от звонка до звонка”. Потом его с радостью приняли в СССР, наградили званием Героя Советского Союза и после его смерти похоронили на мемориальном Новодевичьем кладбище. Сталин ненавидел Льва Давидовича всеми фибрами своей кавказской души, хотя когда-то он даже и объединялся с ним против “плохого” Зиновьева. Главную ненависть И.В. вызвала книга Троцкого о Сталине, где, конечно, многое не соответствовало тому, как советский народ должен был понимать биографию И.В. и ряд его великих деяний. Правда, и сам Л.Д. был далеко не ангел и пролил много крови в период гражданской войны, когда правил после революции почти наравне с Лениным. Так что, можно считать его убийство заслуженной карой, хотя, конечно, политический терроризм находится в ряду тёмных деяний. В худшем положении оказались организаторы этого теракта – Этингон и Судоплатов, которые отсидели достаточно долго в советской тюрьме уже в хрущёвские времена. Ещё одним из героев этой драмы стал незадачливый террорист, выдающийся мексиканский художник и большой Друг СССР – А. Сикейрос. Он тоже попытался было немного раньше, по заданию ОГПУ, покончить с Львом Революции. Как рассказывают в музее Троцкого, он сколотил группу автоматчиков, которые изрешетили дом Троцкого очередями из автоматов (не калашникова, правда). Но опытный конспиратор Лев Давидович спрятался с женой под кроватью и остался пока жив. Бедный же мастер кисти А. Сикейрос был арестован и отсидел в мексиканской тюрьме лет 10-15 (не помню точно), так и не признавшись в заказе из Москвы.

Не могу не отметить и фантастический “серебряный” город Таско, расположенный в нескольких сотнях километров от Мехико. Там раньше добывали серебро и отправляли его в Испанию, а сейчас здесь осталось только множество “серебряных магазинов” для туристов. При подъезде к городу, с дороги нам, вдруг, неожиданно открылась гора и на ней город – фантастика (где только люди не живут!). Приехав, мы сразу же окунулись, но не в атмосферу испанского городка, а в бассейн и наблюдали прямо из воды вид на город, как театральную декорацию. Узенькие улочки с великим множеством лавочек, магазинчиков и магазинов (кошмар!), куда усиленно зазывают покупателей. В центре красивый, обильно украшенный собор начала 18 века. Вдруг, хлынул дождь и по улице побежали вниз потоки воды. Однако, мы, все же, успели купить там небольшие серебряные украшения и сувениры пока не промокли.

Рядом с посёлком Текила находится и потухший вулкан с таким же названием. Как-то я со своим коллегой – мексиканцем выбрались для поездки к этому вулкану. Последние километры грунтовой дороги с рытвинами и камнями, а также крутыми поворотами были весьма трудными для моего “Chevy” и мне часто приходилось тормозить. Наконец то, мы остановились где-то на отметке 4000 м, а высота вулкана около 4500 м. Неожиданно, мы увидели, идущую пешком, группу туристов – мексиканцев. Заметив нас, они с удивлением воскликнули: “О, Chevy!”. Однако, впереди нас ждали еще более серьёзные ис-

пытания. Начав спускаться и притормаживая на крутых участках, я вдруг почувствовал, что педаль тормоза вдруг проваливается в пол, а автомобиль при этом продолжает все быстрее и быстрее двигаться. Я схватился за ручку ручного тормоза, а мой коллега вывернул руль (чтобы сильно не разогнаться) и мы, влетев в кусты, остановились. Ух!!! Не хотелось бы слететь вниз с такой крутой горки… Мы не понимали- в чём тут дело? Совсем недавно я проходил техобслуживание ("Montenimento") автомобиля с проверкой тормозов – и что же делать дальше? Удержит ли "ручник" на крутых спусках и не спускать же даже наш миниатюрный Chevy, придерживая его сзади за бампер (шутка). Подождали полчаса и о радость – торможение восстановилось, проехали немного – опять отказало и так раза два-три. Наконец то выехали на ровное шоссе и благополучно покатили домой. В автомастерской мне ничего не смогли объяснить. Всё оказалось в порядке. Только потом, один мой знакомый автомобилист, сказал мне, что при многократном торможении, которое нам приходилось постоянно выполнять даже и при подъеме, часто закипает тормозная жидкость и тогда тормоза вообще перестают работать! Никто нам раньше ничего такого не говорил, что было бы особенно уместно в горной стране – Мексике. (Господа автомобилисты, путешествующие по гористому рельефу, имейте в виду такое свойство тормозной системы и тогда, возможно … останетесь живыми!).

Сравнительно недалеко от Гвадалахары, на берегу Тихого океана, находится городок San-Blaz, хотя мы и остановились не в нем, а лишь в 15 км от него в уютном отельчике, стоящем в 30 м от линии океанского! (не морского) прибоя. В воде было много мелких перламутровых раковин и их добытчиков из местных жителей и туристов. Однако, главная наша цель это был не San-Blaz, а река … с крокодилами и мангровыми деревьями. Туризм здесь поставлен на речной поток. Приехав на место, мы тут же наняли моторную лодку с лодочником-гидом за 275 peso и покатили по реке la Tobaro. Почти сразу же въехали в тоннель, образованный мангровыми деревьями. Сплетение корней-веток тут такое, что и с мачете не прорубиться наружу, то есть в сторону от реки. Выехав из тоннеля, поплыли по довольно чистой и узкой речке. По берегам иногда попадались кучки черепах, размером до полуметра в диаметре каждая, которые при нашем приближении с шумом плюхались в воду. Вскоре появились и крокодилы длиной метров до двух, лежащие на корягах, рядом с черепахами и в мирном содружестве с ними. У истока реки находился небольшой пруд с чистой водой, который был отгорожен от "крокодильей реки" простой металлической сеткой. В этом пруду мы с удовольствием купались, не думая, что вот за этой небольшой оградой нас могли ожидать, на что-то всегда надеющиеся, страшные животные, а зря… (Вернувшись в Cin, я посоветовал моему коллеге и его жене посетить это интересное место. Они взяли и поехали. Однако, во-первых, его жену в океане "пострекали" какие-то гнусные медузы, так что она ещё месяц после этого болела. Кроме того, когда они купались в устье "крокодильей реки", одна тварь как-то прорвалась сквозь сетку… Купающаяся публика мигом выпорхнула на берег и, хотя никого не съели, но острых впечатлений, было достаточно много.

Из приведенных ранее описаний моих поездок по Мексике может показаться, что вся наша жизнь там состояла из сплошных увеселений и путешествий, но это, конечно, не так. Мы могли отдыхать только в выходные и в праздничные дни. В рабочие же дни мне приходилось проводить занятия. Готовиться к ним, рисуя к каждой лекции по два десятка слайдов, проверять домашние работы студентов, а главное – писать научные статьи на English для международных журналов или конференций. Нужно было также изучать испанский и совершенствовать английский язык, участвовать в кафедральных и университетских мероприятиях, не говоря уже о необходимости всякой хозяйственной работы и главное покупки продуктов, тем более, когда я жил один. Забыл упомянуть, что во второй половине моего пребывания в Мексике я делал доклад на международной конференции по информационной безопасности в Испании. Материал этого доклада относился к обобщению известной теоремы Маурера об усилении секретности. Маурер был учеником моего friend of mine J. Massey, который, кстати, рекомендовал для представления наш доклад с Туркиным в Брайтоне. Джим был очень приятным человеком и автором одной криптосистемы. Я неоднократно встречался с ним на конференциях и помню, что когда я был на “North Cryptoschoole” в Бергене, мы с ним ходили пить пиво в одном из городских баров. Так вот, в докладе, представленном в Испании, мне удалось несколько преобразовать теорему Маурера так, чтобы избавиться от условия ее справедливости только с некоторой вероятностью. Сама конференция проходила в Малаге на берегу Средиземного Моря. Место это мне не очень понравилось – унылая асфальтовая дорожка параллельно линии пляжа и свечки отелей с другой стороны этой дорожки. Море здесь было мелкое и мутноватое. Так что искупался я только для “галочки”. Зато будучи на пересадке в Мадриде и даже переночевав там одну ночь, я смог посетить замечательный музей Prado и посмотреть тамошние картины. На обратном пути из Малаги в Мадрид (для вылета в Мехико) я заскочил на день в Барселону. Этот город конечно замечателен во всех отношениях и, прежде всего, знаменитым “недостроем” архитектора А.Гауди под названием “Sagrada familia”. Однако, в целом, он показался мне слишком интернациональным и поэтому мало испанским.

Наконец хочу остановиться на описании наших поездок в Мексике на океаны и, прежде всего, на Тихий Океан (Pacific).

Первый раз мы поехали на Тихий океан через Акапулько (вспомнилась тогда песня Л. Вайкуле “О, Акапулько, ай-яй-яй…”), но он нам не понравился – слишком много народу, высятся бетонные отели, много машин, пляж самый заурядный и “запипленный”. Со скалы “Cebrada” подростки прыгают за деньги в океан, по пляжу шастуют торговцы сувенирами, прилипая к тебе намертво. Поэтому мы проехали на своём “Chevy” немного дальше по побережью, где одним за другим прячутся в зелени отели классом от 5* до 3*. Наш зарезервированный заранее отель (“Villa Mexicana”) был в ряду последних. В этом уютном, уединённом отеле, в 50 м от берега мы с радостью провели 5 дней. Купались в океане, если удавалось преодолеть прибой, бродили по берегу, летали за катером на парашюте. На это развлечение сначала решилась М., а потом уж и я соблазнился. Оказалось, что дух совсем не замирал и было очень приятно парить над

океаном и береговой полосой метрах в 10-20, а потом плавно опуститься на самую кромку песчаного пляжа. Вечером в ресторанчике на берегу океана зажигали толстые свечи на каждом столе, а на дорожках около домиков – разноцветные фонари. Мы сидели, попивали пиво или коктейли, заедая их морепродуктами и всё это под рокот настоящего могучего океана почти у наших ног. Удивляло и то, что мы, далеко не миллионеры, но могли себе позволять такой отдых даже каждый год. Возвращались в Мехико по хорошему шоссе, наблюдая по сторонам неприхотливые мексиканские деревеньки, но что удивительно – почти у каждой было своё футбольное поле! Вот почему мексиканская футбольная команда "вышибла" команду наших "миллионеров". Поэтому на чемпионате мира по футболу 2018 г, я болел именно за мексиканцев, а не за "наших".

Другое место на берегу океана, которое нам понравилось, было Playa de Ventura. Оно представляло собой небольшой посёлок, точнее ресторанчик с окрестными хибарами, хозяйка которого сдавала апартаменты в домике на самом берегу (метров 30 от кромки воды). Мы жили там несколько дней, столуясь, в основном, вкуснейшим жареным hachinanga (морской окунь) в этом или в ближайшем ресторанчике: 3-4 пластиковых столика под навесом. Всё это время был слышен рокот океана – а это валы длиной до 500 м и высотой 2-3 м, которые с рёвом и завихрением обрушиваются на берег. Бывало ночью, проснёшься и кажется, что сейчас эти волны тебя накроют и снесут вместе с кроватью – а вдруг пришло настоящее "цунами"…? Купаться в таком прибое было довольно опасно, даже если тебе повезёт, и ты прорвёшься сквозь этот прибой в открытое море, то как вернуться обратно? Но мы всё равно купались и не один раз, хотя острых ощущений было с избытком. Для более же спокойного купания ходили километра за два в бухту, где волны не такие страшные, всего 1-1,5 м. Там брали напрокат доски, уходили подальше от берега, ловили волну и иногда мчались на ней к берегу – вот это был кайф! И то я там умудрился свалиться с гребня волны, плавая лишь на "грудной" доске. Волны меня закрутили и некоторое время я не мог даже сориентироваться – где море и где берег… После решил так больше не экспериментировать, а то вернёшься в Россию в гипсе и все будут считать тебя не героем в 63 года, а недоумком – "как дёрнул его чёрт поехать на эти галеры", как говорил один персонаж спектакля питерского БДТ. Интересно, что несмотря на обильное меню из морепродуктов, самым вкусным оказался … морской окунь. Вот так (прекрасное-то рядом!). К сожалению, я привез из этой поездки не только сильные впечатления об океане, но и болезнь живота, которая меня докучала целый год.

Однако, изо всех мест для отдыха на океане, нам больше всего понравилась "Puerta Vallarta" (в переводе "открытая дверь") – это небольшой город на берегу Тихого Океана, примерно в 400 км от Гвадалахары. Мы заказали отель, конечно же, не в самом Puerta Vallarta, а в 15 км по берегу, где нет надоедливой туристической инфраструктуры. Приехав туда, мы нашли, что расположен этот отель очень живописно – в гуще зелени и почти на берегу океана, правда, сам берег оказался заваленным большими камнями, размером в метр – два. Номер был не шикарный, но вполне пристойный и недорогой (кажется всего

30-40 USD за ночь). Наш балкон висел близко к кромке прибоя. Во время шторма и грозы можно было выйти на него и наслаждаться грандиозным зрелищем бушующих волн и пронизывающих их молниями… (Кстати, в 1964 г. в этом отеле снимался известный фильм “Ночь игуаны”, в котором главные роли исполняли суперзвёзды тогдашнего Голливуда – Ава Гарднер и Ричард Бёртон. В этом фильме была рассказана романтическая история, возникшая между одной туристкой из группы учителей (её играла другая актриса) и экс-священником, живущим в Пуэрто Вайярте.)

Мы сразу же поняли, что купаться рядом с отелем невозможно из-за громоздких камней и опасности прибоя и поэтому с утра отправлялись искать более удобные места и, конечно, посмотреть окрестности. Сначала шли по шоссе, проложенному в гористой местности среди густой тропической зелени. Вышли к речке, впадающей в океан, где “полоскалось” множество лодок. Одну из них (с моторчиком) мы наняли, и лодочник повёз нас вдоль берега до другого прибрежного обитаемого места, километрах в 2-х – 3-х. Пока плыли, восхищались красотой прибрежной полосы, покрытой густой тропической зеленью, среди которой выделялись кокосовые пальмы, а вся местность была гористой, или, скорее холмистой. Нам казалось, что это очень похоже на какой-нибудь остров в Полинезии, где мы, правда, никогда не были и, думаю, уже не будем. Увидев, что дорога не только проходимая, но и привлекательная, мы обратно пошли уже пешком по тропе, проложенной в зарослях. На следующий день повторили весь маршрут тоже пешком; шли не торопясь, останавливаясь в уютных бухточках для купания и отдыха под пальмами, с которых свисали большие кокосовые гроздья. (Мы тогда ещё не прочитали в местном справочнике, что на всём океанском побережье Мексики (длиной около 10 000 км) от акул погибает в среднем за год 1-2 человека, а от падения кокосов на голову… около 100 человек!) Проходя вдоль кромки воды, с удивлением наблюдали метрах в 100 от берега резвящихся китов. Их морды то выскакивали, то погружались (по дуге) в воду, а последним зрелищем были огромные, вертикально стоящие хвосты, которые потом медленно-медленно исчезали в воде.

Вот так, почти в “тропическом раю” мы провели 4 дня, питаясь в небольших ресторанчиках и попивая через соломинку-тростинку, так называемое, “кокосовое молоко”, которое на самом деле, прозрачно и очень хорошо утоляет жажду в жару. Вернулись в Гвадалахару к вечеру, хотя выехали с утра – всё же 400 км, хотя и неплохого шоссе, но достаточно гористого и петляющего в зелени. Наблюдали по дороге много голошеих грифов, которые сидели на невысоких деревьях, ожидая, что вдруг кто-нибудь, да и сдохнет… Иногда я думал – что такое “рай на земле?” – это работать и жить в Гвадалахаре и каждый “week-end” приезжать на вулканический пляж на берегу Пацифика, купаться, наблюдать за прибоем и пить кокосовое молочко из трубочки, вставленной в плод… Вот почему, многие и далеко не бедные, американские пенсионеры покупают себе дома в Мексике и уезжают туда в завершение своей земной US-жизни. Правда, преступность…, но тогда они поселяются в городках, огороженных высоким “muralem” (стеной), где проезд и проход только по пропускам, а там внутри – поля для гольфа, охранники, корты и другие западные радости.

Наконец, ещё одно место отдыха на океане, которое нам очень понравилось это Карибы, т.е. часть Мексики, омываемая Карибским морем. Самый известный курорт этого района это, конечно, Cancun, который мы, правда, постарались проигнорировать, как “местечко с небоскрёбами”. Мы же поехали на остров Cosumel. (У нас даже сложился свой куплетик после моей напряжённой работы в Cin: “Прощай моя работа, дела и канитель, мы завтра улетаем на остров Cosumel”!) Долетели самолётом до Канкуна и потом час еще на пароме плыли до этого острова, причем эта поездка запомнилась нам негативно. Дело в том, что после шторма в океане появились крупные волны. Хотя паром был достаточно большим (на нём даже перевозилось около десятка автомобилей), но качка выдалась весьма заметной. Сначала это даже развлекало пассажиров. Они при подъёме на каждую волну и последующем падении вниз начинали хором скандировать: “О…, О…, Ах”. Но потом таких энтузиастов становилось всё меньше и меньше и звуки стали другими: “ры... ры... ры”. Хорошо еще, что плавание было недолгим (около часа). Высадились мы при сильнейшем тропическом ливне, прячась под зонтами и шагая к отелю прямо по потокам мчащейся по улице воды. На утро уже светило солнце и, взяв в аренду автомобиль “Жук” (Folkswagen), мы отправились по острову, величина которого была столь мала, что смогли весь его объехать еще до обеда. Море на Карибах это ярко бирюзовая и прозрачнейшая вода, пляж – из чистейшего и мельчайшего вулканического песка. По дороге наблюдали фонтанирующие при прибое “гейзеры”, красивые вулканические скалы и даже попался мёртвый питон, причем в течение нашего “путешествия” людей мы практически не встречали. “Гринго” сосредотачивались, в основном, возле невысоких прибрежных отелей, купаясь в бассейнах (“не лезть же в это сомнительное море…!”) или в дельфинариях, наблюдая за трюками дельфинов, а иногда даже и участвуя в них. На следующий день мы собрались на морскую (океанскую) прогулку для плавания со snorkel (т.е. с маской и трубкой). Высадили (выбросили) нас примерно в километре от берега, около кораллового рифа (по красоте, занимающего второе место после австралийских рифов). Тут-то мы и увидели сквозь маску настоящие океанские красоты: стаи радужных рыбок (“ангелы” и др.), вьющиеся в скалах мурены и где-то внизу проплыл огромный “eaglray” (т.е. скат). Было такое впечатление, что мы для себя открыли совершенно новый мир. Конечно, проплывшие где-то там внизу аквалангисты, видят намного больше, но всё же и платят за это большую цену, чем мы, так сказать, “подводные матрасники”… Пробыв на острове дня 4, мы получили огромное удовольствие и массу новых впечатлений.

Тут я впервые попробовал водить “жука” (это, кстати, тогда было наиболее распространённое такси в Мексике). У меня на нём, при переключении передач, появлялось такое ощущение, как будто я чувствую подряд все его скрипящие металлические сочленения, идущие от руля к колёсам.

Теперь, когда кто-нибудь описывает морской отдых на Средиземном море или в Греции, где мы и сами не раз бывали и называли это место “эгейщиной”, я хвалю и умиляюсь, но ни разу не встретилось нам (включая и атлантические пляжи в Португалии) такой красоты, чистоты и даже уединённости, как

на тихоокеанских пляжах Мексики и всё это было в 4-5 часах не очень быстрой езды от нашей квартиры в Гвадалахаре или в 5-6 часах, но еще более быстрой езды, от нашей квартиры в Мехико.

Мое пребывание в Мексика подходило к концу и осенью 2002 г. я должен был отбыть в alma mater. Наверное, я мог бы остаться еще здесь и поработать в каком-нибудь другом университете, пусть даже и за меньшую зарплату. Взглянув правде в глаза, я не могу сказать, что в Cin пожалели кого они в моем лице потеряли. Думаю, что им было глубоко безразлично мое присутствие среди их профессоров. А о том, как я от этого только выиграл, скажу, что помимо личных соображений (лечение глаз в Федоровском центре, который намного лучше мексиканского, покупка и обустройство новой квартиры для проживания во втором браке и т.п.), мне несколько поднадоело каждый день ходить “от и до” на работу, строчить статьи независимо от их важности и настроения и, наконец, я хотел еще поездить по миру не только как турист , но и как научный работник и лектор, который совмещает полезное с приятным, а это в Мексике было бы не просто сделать.

6. Постмексиканский период

Вернувшись в Питер, я еще до конца года поработал старшим научным сотрудником у моих знакомых на предприятии “Вектор”, а затем с начала нового семестра продолжил “сеять доброе и вечное” в должности профессора кафедры информационной безопасности Бонча. Продолжал читать там лекции и проводить групповые занятия, а также руководить дипломниками и аспирантами. Конечно, существенную часть моего времени, да и моих интересов, занимала научная теоретическая работа по направлению стеганографии и ЦВЗ. Еще будучи в Мексике, я познакомился там с одним профессором из французского университета ENST, который тогда был на некоторой время приглашен в Cin и договорился с ним о приглашении меня в качестве Visiting Professor на месяц в будущем году. Это привлекало меня еще и потому, что этот университет был расположен в живописной местности на берегу атлантического фьорда, недалеко от французского города Бреста, в Бретани.

Во время моего визита в Бретань я прочитал там несколько лекций, в том числе по обобщенному алгоритму Витерби. Идея последнего пришла мне много лет назад, и я тогда даже переписывался по этому вопросу с самим А. Витерби, хотя он, мне кажется, не считал этот мой алгоритм существенным продвижением своего, а просто некоторым обобщением известного результата. Однако, это позволило мне в одной работе с моим аспирантом [13] легко применить данный метод к каналам, как с межсимвольной интерференцией, так и с замираниями и кодированием. Кроме того, один из сотрудников ENST занимался тематикой ЦВЗ и поэтому у нас было общее направление для совместного обсуждения. Поселили меня в отдельном коттедже на кампусе университета с видом на фьорд. Вдоль этого фьорда шла тропа по травянистым холмам, по которой можно было за полчаса дойти до небольшого городка с бухтой. Я иногда гулял по ней в выходные и вечером после работы. Местные жители мне говорили, что во время немецкой оккупации, в этом фьорде, а точнее в глубоких тоннелях,

отходящих от него в глубь скал, прятались немецкие подлодки, нападавшие на американские конвои. Обедал я в университетской столовой, где меня, как всегда, поразила сравнительная дешевизна обедов и, имеющееся в ассортименте, сухое красное вино (тоже дешевое). Вот что значит французы – им небольшая выпивка в учебе не помеха. На будущий год удалось повторить такой же визит, воспользовавшись тем обстоятельством, что в Питер вскоре приплыло французское судно "Жанна Д'арк", на борту которого находился ректор ENST и при его посещении Бонча, я выступал переводчиком (с английского) между ним и нашим ректором Г. Во время моего второго пребывания в этом университете помимо работы я много играл в теннис с моим поступившим уже в аспирантуру протеже из Одессы. Это возможно сыграло отрицательную роль в рецидиве моей болезни с головокружением, что диагностировалось как транзиторное нарушение мозгового кровообращения.

После окончания моего второго пребывания во Франции ко мне приехала моя жена М. и мы поселились в коттедже, пригласившего меня профессора Б., а он со своей женой и дочкой приехал через некоторое время в Питер и жил в моей квартире, тогда как я уехал на это время на дачу. (Замечу, что обмен на время квартирами – это было весьма популярной опцией в то время, так как экономит самые большие деньги при посещении другой страны, а именно деньги на отель.) Во время небольшого недельного отдыха на берегу фьорда мы с М. наслаждались прогулками по скалистому берегу с фантастическими многометровыми приливами, а, главное, посетили остров Quessant, расположенный примерно в 30 км от берега, в Атлантике. Там находится небольшой поселок, а берега с бухтами и живописными нагромождениями скал особенно хороши были при сильном прибое. Имел ли я затруднения с французским языком? В ENST практически нет, поскольку все преподаватели и администрация знала более – менее, английский. Но вот при разговоре с местными жителями (как куда-то пройти?) возникали трудности, особенно при общении с возрастными людьми, в то же время, я не заметил какого-либо негативного отношения к английскому языку. Перед первой поездкой во Францию я в течение пары недель брал уроки французского, но, конечно, кроме некоторых правил чтения и "здравствуйте", "до свиданья", "спасибо", "хорошо", "плохо", почти ничего за это время не удалось усвоить.

Замечу, что до ENST я добирался на автобусе от г. Бреста, а туда ехал на скоростном экспрессе TZV из Парижа. Конечно, невозможно было проскочить этот город, не посетив Лувр, Нотр-Дам, Сен-Шапель и не прогулявшись по Елисейским полям с посещением местных кафе. Я даже подстригся (на память) в одной из парижских парикмахерских, чтобы потом удерживать в России парижскую прическу.

Будучи на недельном отдыхе после моих лекций, в коттедже Б. мы с М. также посетили живописный новодел San-Malo, а также подлинный шедевр – замок на острове Мон-Сен-Мишель и, наконец, Ренн с его парком роз.

Вернувшись в Питер, я продолжил чтение лекций по основам стеганографии и руководство несколькими дипломниками и аспирантами. К сожалению, мои головокружения, случавшиеся во Франции, в Питере не ушли, а наоборот

усилились, да причем до такой степени, что я “загремел” в больницу “Святой Елизаветы”, где и провел две недели. После этого симптомы ушли, но, увы, вернулись, когда я работал в Португалии, но об этом чуть позже.

Примерно в это же время мне присвоили звание “Заслуженного Работника высшей школы Российской Федерации” с удостоверением, имеющим факсимиле Президента РФ.

Вскоре наш университет посетил профессор Ли из Южной Кореи и предложил мне приехать туда в университет Chonbuk аж на целый семестр, чтобы там прочитать и поставить курс “Information Hiding”, что я и сделал в 2005 г. Город Чонбук небольшой, он находится километрах в 200 к югу от Сеула и знаменит, разве лишь, своим университетом, где учится довольно много студентов, причем из разных стран. Довольно много китайцев, есть и русские, которые перед этим изучали корейский язык, хотя преподавание почти всех предметов ведется на English. Так случайно оказалось, что я приехал одновременно с одним профессором-математиком из МГУ. Он читал курс по эллиптическим кривым и связанным с ними кодам. Поселили нас на кампусе в разных небольших комнатах, расположенных друг напротив друга. Мы могли бы снять, конечно, оплачиваемое жилье и в городе, причем с оплатой покупки мебели и самых необходимых личных вещей. Однако, предпочли находится ближе к университету, да и деньги, выделенные на обустройство, удалось взять в дополнение к гонорару. Вообще оплата нашего пребывания была выше всех похвал. Это и профессорский гонорар и подъемные и оплата авиа билетов. (Больше, чем в Корее мне нигде не платили!) С моим коллегой мы конечно общались, причем чем дальше – тем … хуже. Он оказался довольно тяжелым на подъем, довольно занудным, а, главное, близким к идеям ушедшего уже от нас социализма-коммунизма. Студенты (их было в моей совместной с ним группе человек 25) оказались довольно внимательными, хотя и не всегда вовремя выполняли мои задания по home work. Работать приходилось с использованием компьютерного проектора и заранее привезенного мной цифрового курса лекций на English, хотя кое-что, конечно, нужно было и дорабатывать. В неделю было обычно три пары, то есть 6 часов занятий. Помимо учебных занятий, приходилось заниматься и разработкой научных статей. Наш приглашающий профессор был в этом отношении строго заинтересованным – мы должны были за семестр написать и представить в международные журналы не менее двух “совместных с ним” статей, каждый. Но проблема заключалась в том, что, конечно, саму публикацию этих статей следовало ожидать много позднее. Так у меня с Ли вышла “совместная” статья только в 2006 г. [14] и доклады на международных конференциях [15]. Так что пришлось нашему профессору поверить мне, так сказать, в долг. Кроме того, он очень ревностно следил за нашими занятиями и научной работой. Почти каждый день звонил нам на наши рабочие места и проверял, там ли мы? Даже иногда в выходные он удивлялся, если нас не было на работе. Однако, мы старались его не приучать к нашему присутствию на работе в эти дни, если в этом не было острой необходимости – иначе мы вообще ничего не смогли бы посмотреть в новой для нас стране. В самом городе Чонбук смотреть-то особенно было нечего – разве лишь такую корей-

скую экзотику, как кипящие чаны с какими-то желтыми толстенными червяками или магазины с местными художественными промыслами. Поэтому я старался в каждые выходные поездить по стране в одиночку или с группой экскурсантов. Так я побывал в нескольких буддийских монастырях и в “Городе … любви” (он так назывался не из-за доступности жриц любви, а по каким-то историческим соображениям). Посмотрел я цветение знаменитой сакуры (хотя это и бренд Японии). Был в музее девушки-героини, которая во время оккупации Кореи японцами влюбила в себя японского генерала и когда он совсем уже разомлел, обняла беднягу и бросилась с ним с обрыва. (Думаю, что и у нас во время ВОВ нашлась бы такая героиня, хотя обрывы большие у нас не часто находятся под рукой…) Вообще, корейские девушки не блещут красотой на наш европейский вкус, но встречаются такие (и я их видел!), что глаз не оторвать и, как правило, они с удовольствием общаются с иностранцами. Особенно примечательной была моя поездка (во время недельных каникул) на субтропический остров Чеджудо. Пришлось лететь туда самолетом, резервировать отель и вписываться во всякие туры. Там мне попалась группа со “стайкой девушек в цвету” – см. М. Пруста. С ними я поднимался на какую-то довольно высокую гору (вроде бывшего вулкана) и потом с одной из участниц мы еще некоторое время переписывались по Интернету – она жила со своими бойфрендом в Сеуле. Скажу еще пару слов о корейской кухне, которая у нас в России довольно слабо представлена. Но тут она, конечно, была доступна в полной мере. Честно говоря, я ее не любил в Росси и не полюбил здесь. Кстати, когда я только что приехал на автобусе из Сеула в Чонбук, то на автовокзале нас двоих встретил проф. Ли и сразу же повел в вокзальный ресторан, причем там почему-то было очень сумрачно. Я, будучи довольно голодным после многочасового перелета, набросился на нечто в тарелке и довольно переперченное. Эта неосторожность потом заявляла о себе болью в животе несколько дней. В университетской столовой я стал более осторожным и по началу выбирал только какой-то жидкий суп и рис. Потом немного приспособился, но всегда смотрел на меню с подозрением. Впрочем, в магазинах в городе всегда можно было купить что-нибудь европейское-обычный хлеб, колбасу, сыр, сосиски, чипсы и т.п. Можно было выпить и неплохое пиво, но только не корейскую водку “Суджу” – это для меня была чистая отрава. Я спрашивал коренных корейцев, почему они все так наперчивают? Злые языки говорили, что в древности корейцы жили очень бедно и поэтому им приходилось есть испорченные продукты – вот они их и наперчивали, чтобы не заболеть. Правда, сами корейцы этот миф отрицают также, как и тот, что они любят, будто бы, попробовать собачатину. Впрочем, еще кто-то мне говорил, что по сговору с хозяином, в некоторых ресторанах ее можно и заказать… (Хотя, что тут брезговать – собачка на вид будет почище свиньи, только их просто жальче...) Познакомился я там с одним профессором из Индии, и мы с ним ходили на выступления корейских моделей и в кино. Он приглашал меня приехать с лекциями в Индию, но как-то не получилось. После почти 4-х месячного пребывания и преподавания в Корее мне уже как-то захотелось домой, хотя типично я не слишком ностальгирующий человек, что доказывает мое более чем трехлетнее пребывание в Мексике, при-

чем, большую часть времени в одиночестве. Вот мой коллега из Москвы очень хотел уехать из Кореи, но у него контракт был заключен еще на семестр и поэтому он мне очень завидовал.

Чтобы немного снизить градус райской жизни в Корее, скажу, что все же жизнь и преподавательская работа в чужой стране – это не совсем сахар. Все время находишься в некотором напряжении и в большой ответственности – а вдруг не угодишь студентам или принимающему профессору. Кстати, подготовить (и потом напечатать в международном журнале) за один семестр три работы, это не так уж и мало по техническим наукам. Например, в мексиканском, университете, где я раньше работал, одна статья в хорошем иностранном журнале в год, считалась неплохим результатом. Кто-то из корейских профессоров (возможно и из завистников Ли) сказал мне, что у него, то ли 200, то ли 300 печатных работ и большинство из них в соавторстве с приглашенными иностранцами. Кстати, Ли подарил мне свою небольшую, написанную им книжечку, в которой он доказывал, что стеганографию изобрели именно древние корейцы. Будто доподлинно известно, что один корейский крестьянин (тоже конечно Ли) когда уезжал в город, то клал справа от своего дома большой камень, а когда он шел в соседнюю деревню, то клал тот же камень, но уже слева. Чем не стеганография, да еще и “стеганография вещей”?!

Вернувшись в Россию, я продолжал заниматься рутинной преподавательской работой и более интересной работой с аспирантами. Так с одной моей аспиранткой К. мы разрабатывали тему “Стеганография в каналах с шумом”. Насколько мне было известно, никто больше в мире этим направлением пока не занимался, а стоило бы… Действительно, если обнаружение присутствия СГ происходит уже при наличии какого-то шума, то возникает ряд особенностей, которые значительно повышают стойкость таких систем к их обнаружению и, кроме того, в отличие от СГ в бесшумных каналах, можно обеспечить их необнаруживаемость даже при точном знании покрывающих объектов (ПО). Мы с ней опубликовали несколько работ (например [16]) и в итоге она написала и успешно защитила кандидатскую диссертацию. Жаль только, что в дальнейшем, хотя она и перешла работать преподавателем на нашу кафедру, но научную работу у нее заслонила демографическая проблема, более актуальная для РФ.

В 2005 г. мне удалось посетить международную конференцию, посвященную разработке систем ЦВЗ в г. Сиенна (Италия), где я делал доклад о возможности построения необнаруживаемых стегосистем для каналов с шумом. На этой конференции присутствовали два наиболее известных специалиста в мире по разработке стегосистем – это J. Fridrich (США) и M. Barni (Италия), с которыми мне удалось побеседовать по интересовавшим меня проблемам. Вообще, доклады на этой конференции были не очень интересными, на мой взгляд, но сам город Сиенна – выше всех похвал, поскольку это город 15-16 века, сохранивший местами историческую архитектуру и имеющий музей с итальянской живописью. Типичным моим поведением на этой конференции было посещение некоторых, интересовавших меня докладов, а затем я отправлялся в ближайшую тратторию, чтобы заказать у знакомого мне уже бармена стаканчик Кьянти (ценой в одно лишь евро!) Банкет по окончанию конференции тоже

проходил в старинном зале, стены которого были украшены яркой итальянской живописью.

Конечно, оказавшись в Италии, я не преминул охватить другой замечательный объект – город Флоренцию с его известным собором, а главное, с галереей Уффици, куда я заранее по интернету заказал себе билет – иначе бы и не попал туда из-за большой очереди. Кроме того, я не смог отказать себе в удовольствии, находясь в Сиенне, съездить на автобусе в недалекую Пизу, с ее известной падающей башней. Правда, на верх башни мне так и не удалось забраться из-за ее ремонта, но зато я наслаждался внешним видом этой "сахарной головы", да еще и со значительным наклоном. Потом вышел рядом на берег мраморного моря. И, действительно, там лежали огромные глыбы мрамора. Понятно теперь, что именно это стимулировало знаменитых итальянских скульпторов, вроде Кановы.

Один мой бывший аспирант М., с которым мы опубликовали несколько печатных работ в международных журналах и которому я потом дал рекомендации для обучения на Ph.D-туре в Дании, после успешной защиты своих Theses, был приглашен для работы в Японию (Токио) в исследовательский институт AIST. Поэтому я воспользовался его поддержкой для приглашения меня на две недели в этот институт, тем более, что одним из отделов (где уже и работал М.) руководил, известный мне по научным статьям, японский ученый Hideki Imai. Поэтому в 2006 г. я приехал в Токио. В течении моего краткого визита я смог пообщаться с некоторыми японскими учеными, результатом чего явилась подготовка совместной статьи, которая была позже опубликована в весьма престижном журнале Trans. IEEE on IT [17]. Конечно, Япония весьма экзотическая страна. Начиная с вежливости ее обитателей и левостороннего движения, но не только поэтому. Так я жил в типично японской гостинице, где в моей комнате совсем не было мебели – только циновка с постельным бельем, а одежду я просто бросал на пол, когда ложился спать. Конечно, можно было снять номер и в отеле европейского типа, но это было бы значительно дороже (хотя мне суточные и перелет оплачивал AIST, но это было не так уж много) и, кроме того, мне хотелось немного пожить по-японски, тем более, что на моем отельчике горели вечером японские фонарики, а совсем рядом находилось древнее буддийское кладбище. В субботу на соседней площади устраивались стихийные и вполне западные танцы, а на работу я ездил на японской электричке, не было у меня разве только лишь встречи с … "японским городовым". Так как у меня было всего два weekend, то я в один из них посетил знаменитый храм в пригороде Токио, где типично хоронили самураев, а в другой выходной поехал на скоростном экспрессе к подножию вулкана Фудзияма. На сам вулкан проход оказался закрыт и оставалось только любоваться им на расстоянии нескольких километров, вспоминая картины Хокусая – "500 видов горы Фудзи". Обратно я возвращался на стилизованной "пиратской шхуне". После работы много гулял по Токио, который, на мой взгляд, мало чем отличается от европейских городов, много раз ходил по главной улице – Гинзе и даже заказал там и купил для М. ожерелье из жемчуга. Конечно, это был не тот жемчуг, для добычи которого "У острова Курмыза" посылал на дно водолазов безжалостный русский купец, а

тот, что извлекается из раковин, выращенных в искусственных водоемах. Однажды вечером я посетил типично японский театр Кабуки – язык тут не надо было знать, а разыгрываемое содержание подробно описывалось в англоязычной программке. В один из вечеров меня пригласил проф. Imai вместе с несколькими японскими коллегами на party в кафе, где на движущемся конвейере предлагалось, на выбор, множество различных суши и все это потом (уже без конвейера) запивалось зеленым чаем.

Забыл сказать, что в это время я начал более интенсивно интересоваться вместе с моим коллегой по кафедре и бывшим учеником В.А.Я., распределением ключей по каналам связи с шумами. Это одно из поднаправлений бесключевой криптографии, когда секретность распределяемых ключей обеспечивается не криптографической защитой, а свойствами каналов связи. Один из таких подходов состоит в том, что для дополнительной рандомизации канала связи используется антенна со случайно управляемой диаграммой направленности. Позднее по этому материалу была написана моя работа совместно с аспирантами [18], а пока я пытался связаться с одной японской фирмой, чтобы спросить, не могут ли они продать мне такую антенну? После некоторых раздумий их ответ был такой – для РФ нет. (Много лет спустя похожая антенна была реализована в Бонче (правда для других целей) и мы пытались попробовать на ней практически выполнить эксперимент с распределением ключей.)

Возвратившись в РФ, я надеялся, что наш бизнесмен – завкафедры поможет мне в реализации некоторых моих теоретических разработок, таких как СГ, ЦВЗ или распределение ключей по каналам связи, но напрасно. Он послал меня к своему помощнику, а тот “спросил, как отрезал” – могу ли я что-то продавать прямо сейчас, и получив отрицательный ответ, я пошел ... лесом. Почему-то в USA имеется и благополучно работает фирма DigiMark, которая занимается мониторингом и вложением ЦВЗ для заказчиков, а у нас это никого не интересует? Не могли мне помочь в практической реализации своих диссертаций и мои аспиранты, несмотря даже на наличие у нас зарегистрированных патентов, хотя темы были вполне прикладные, например, такие как “Аутентификация цифровых изображений при помощи ЦВЗ” – почему бы не защитить так права интеллектуальной собственности? К сожалению, в это время наметилась неприятная тенденция при обучении аспирантов. Некоторые из них, проучившись в аспирантуре год-два и даже опубликовав со мной несколько интересных работ, уходили, “спасибо не сказав”, причем по разным причинам – девушки детей собирались рожать, юноши жениться или “свалить” за границу на ПМЖ. Конечно, корень всего этого был в низкой оплате аспирантов и отсутствии перспектив приемлемой оплаты даже в ближайшем будущем, то есть на доцентских и даже на профессорских должностях. Напрасно я пытался привлечь их к продолжению занятий наукой своим примером – мол немного поработаете у нас, защититесь, а потом я помогу вам устроиться на учебу или (хотя бы временную работу) за границей. Нет, никто не хотел ждать до завтра. Сейчас или никогда! Через несколько лет наметилась и другая причина нежелания заниматься наукой после окончания аспирантуры и даже после успешной защиты диссертаций – устройство способных людей на работу в различные (чаще всего

в зарубежные) компании, то есть афоризм Резерфорда для своих учеников “Bread, butter but no jam” был, конечно, предложен не для них.

Замечу, что еще одной целью моих поездок за границу было общение с людьми, интересующимися наукой, хотя, конечно, я понимал, что эта черта подпитывается неплохой финансовой поддержкой.

Занимаясь обзором литературы по направлению “Wire-tap channel”, я нашел в журнале IEEE статью одного португальского ученого (J. Barrosa), которая меня заинтересовала, поскольку она была в русле нашей бесключевой криптографии, и, в частности, распределения ключей. Причем, по-моему, он даже ссылался на какую-то нашу статью в этой области. Поэтому я написал ему письмо в Интернете и предложил приехать в его университет в Порто для “collaboration”, если у них такая возможность пригласить меня, как Visiting Professor, имеется? После его положительного ответа, я уехал (улетел) в Порто на месяц в апреле 2008 г. По приезде в университет Порто я прочитал там несколько лекций на кафедре Barros-а и немного обсудил с ним его метод решения проблемы подслушивающего канала с использованием, так называемых, helper-ов. В это же время, именно в Порто, проходил семинар IEEE on IT Workshop, так что я смог посетить интересные доклады и поговорить с участниками, некоторые из которых были из РФ. К сожалению, Barros должен был в это время неожиданно уехать на стажировку в MIT (USA) и поэтому я не смог с ним пообщаться более тесно. Однако, я не очень пожалел об этом, так как только лишь пребывание в живописном городе Порто вдохновляло меня на новые исследования, даже и без тесного общения с его обитателями.

Поселили меня в красивом коттедже, где типично бывали различные государственные приемы. (Так во время моего пребывания там с кем-то встречался даже Президент Португалии.) Мои апартаменты были на втором этаже, куда вела винтовая лестница, тогда как на первом этаже находился небольшой ресторан, где постояльцам отеля можно было заранее заказывать блюда. Мой университет находился в пешей доступности. В свободное от лекций время я, конечно, осматривал гористые улицы этого города, который еще больше украшала река (тоже Порто). По этой реке раньше приплывали для доставки по миру бочки со знаменитым португальским портвейном, а сейчас на берегу располагался дегустационный бар, где можно было попробовать множество сортов этого чудесного (не сравниваю с нашими тремя семерками) портвейна. Совсем недалеко можно было пройти до побережья Атлантики, где находился и порт. Городской вокзал был знаменит своими talaveras, то есть керамическим картинами. Запомнились и небольшие ресторанчики, где подавались разные морепродукты, из которых мне особенно понравилось такое блюдо как pulpo, то есть щупальцы осьминога, приготовленные совсем не жесткими. Однако, моя безмятежная жизнь в Порто, вдруг оказалась нарушенной очередным приступом моего головокружения. Причем ничто не предвещало эту атаку – я шел по крутой улице и вдруг все закружилось и затошнилось, да так, что мне пришлось прижаться к стене дома, чтобы не упасть. Еще надо было как-то защититься и от того, чтобы тебя не приняли за пьяного. Пришлось срочно ловить такси и предохраняясь целлофановым пакетиком, ехать в свой отель. Там я плюхнулся

на кровать, но приступ не проходил. Следующие два дня были выходные и я попытался выползти на улицу и пройти к океану. Сначала вроде полегчало, а потом все началось снова и сильнее, так что я еле добрался до постели. Все выходные пролежал дома с температурой 38, при верхнем давлении 180 и с постоянным использованием гигиенического пакета. Да, болеть за границей – это спаси и сохрани…! После пары дней такого состояния, я, все же, решился и через консьержку вызвал скорую помощь. С сиреной она отвезла меня в больницу (госпиталь по-португальски). Поместили меня, как бывало и в РФ, на койке в ... коридоре (никто не считался с тем, что я профессор из Росси – нет мест в палате – лежи в коридоре). Условия в этой больнице, скажу я вам, не слишком хорошие. Все заполнено больными, да еще и родственники толкутся тут же, рядом с пациентами. Правда, довольно скоро ко мне подошли врачи и на English я объяснил им, что со мной случилось и как я себя чувствую. Померили давление. Сняли кардиограмму и даже рентген мне сделали, так как давления на левой и на правой руках сильно отличались. Дали какие-то таблетки. К сожалению, тут английский знали далеко не все, а мой испанский мало помогал мне среди португальско-язычных. Так я пролежал до вечера почти без диагноза, и тут все мои симптомы исчезли и меня выписали в тот же день, обязав заплатить за лечение 30 евро (потом мне это компенсировали по страховке). Но, конечно, выйдя из больницы, я еще долгое время находился в опасении, что все это может повториться. К счастью, через несколько дней ко мне должна была приехать жена и привести, выписанное в РФ моим знакомым врачом, лекарство (бетасерк), которое я и стал постоянно здесь принимать. Слава Богу, приступы больше не повторялись.

Мы заранее договорились с женой, что после окончания моего “визитерства”, съездим на недельку для отдыха в южную провинцию Португалии Algarve. Так и сделали и, заказав заранее отель, отправились на поезде через всю страну в эту местность на берегу Атлантики. Отель был неплохой и пляж огромный и пустой с повсюду сопутствующими ему песчаными холмами. Однако, наши надежды на загар и купанье в конце мая не оправдались. Оказалось, что несмотря на постоянное солнце, с океана дул сильный ветер и мы (в начале мая) все время замерзали на пляже, прикрываясь даже зонтом, но не от солнца, а от ветра! О купании не могло быть и речи. Только перед отъездом окунулись в холодную воду просто для памяти. (В утешение, нам сказали, что такая погода типична для атлантического побережья Португалии). В течение нашего отдыха на океане мы посетили небольшие и симпатичные городки со множеством сувенирных магазинов и съездили с экскурсией в Лиссабон, где увидели сверхдлинный мост и памятник Колумбу с сотоварищи… Немного прошлись по улицам Лиссабона, попробовав мороженное в португальском кафе. Забыл отметить, что во время нашей несколько-часовой поездки на поезде, мы наблюдали рощи пробкового дуба, хотя издали на дубы эти низкорослые деревья были мало похожи. Известно, что эта страна основной поставщик натуральной пробки в мире, получаемой, как коры с пробковых дубов.

После возвращения из Порто в Питер у меня вскоре появился один аспирант, довольно трудолюбивый, с которым мы начали разрабатывать актуаль-

ную тему “Коалиционные атаки на ЦВЗ” – это когда несколько “пиратов” объединяются, чтобы удалить ЦВЗ из какого-нибудь мультимедийного продукта, например, видео клипа. Такая атака оказывается особенно опасной для собственников этого продукта, так как иногда позволяет сделать для них невозможным извлечение ЦВЗ без ухудшения качества основного продукта. В результате этой работы нам удалось предложить методы защиты от таких атак и опубликовать несколько работ в международных журналах, что обеспечило аспиранту успешную защиту диссертации и получение диплома к.т.н. К сожалению, он после защиты уехал на Алтай, где ему обещали работу и жилье – ну что же- насильно мил не будешь. Еще один мой аспирант К. успешно работал по теме “Изощренные атаки на ЦВЗ”. Мы опубликовали по этой перспективной теме несколько интересных статей, но он вдруг неожиданно исчез “спасибо не сказав”. Через год объявился, чтобы по телефону извиниться, а то, что он тему “затоптал и бросил” – это как называется?

Одна из моих последних дальних поездок с научными целями, но не только, была поездка (в действительности, конечно, дальний перелет) в Сингапур. Она была организована также при поддержке моего бывшего ученика (уже упоминавшегося мною ранее К.М.), который в это время работал в Токио. Там вместе с ним работала одна ученая дама из Европы, которой он и замолвил словечко за мою персону, поскольку эта дама переезжала работать в Сингапурский университет Nanyan. Мой случай не был исключительным. Действительно, приехав в этот университет, я обнаружил, что там работает по временным контрактам довольно много ученых из Европы и из США – это у них оказывается традиция такая, что и позволяет постоянно поддерживать достаточно высокий уровень научных исследований, не прибегая к стимуляции под лозунгом “догнать и перегнать”! Данная поездка оказалась довольно плодотворной, поскольку, во-первых, я познакомился там с одним профессором из Bell System, который показал мне свою давнюю статью по построению системы ЦВЗ. По приезде в РФ, я предложил ее усовершенствовать одному моему аспиранту А. К., чтобы сделать ЦВЗ устойчивым против целого комплекса атак. Итогом оказался ряд наших совместных с аспирантом печатных работ и успешная защита его диссертации. Что же касается второго случая, то проходя как-то по лаборатории этого универа, я обратил внимание на одного Ph.D.-ка из Германии, который собирал схему для извлечения ключа из невскрываемого чипа шифратора с использованием утечки по цепям электропитания. Вернувшись в Россию, я стал подробно разбираться с этим направлением. Вообще-то, перехват информации по побочным каналам, и, в частности, по цепям электропитания не являлся для меня новостью. Однако, тут использовался новый подход – так называемое DPA (Different Power Analysis). Фишка такого подхода состояла в том, что удавалось по частям извлекать биты ключа, контролируя форму колебаний на сопротивлении в цепи питания и максимизируя взаимную корреляцию при известной схеме шифрования. В отличие от ранее известных методов анализа по побочным каналам, данный подход был пригодным даже при наличии дополнительного зашумления, поскольку требовал тогда лишь некоторого увеличения времени анализа. Данное направление исследований я предложил, как

тему диссертации одного моего способного аспиранта. Успех превзошел все мои ожидания. Проработав два года с макетом в одном из государственных институтов и используя зарубежный АЦП, купленный за USD, аспирант доказал теоретически и экспериментально, что можно в обозримое время найти ключ, извлекая его из невскрываемых чипов шифрования/дешифрования и предложил методы защиты от такой атаки, который мы и опубликовали в научном журнале [19].

Немного расскажу о моей жизни в Сингапуре. Поселили меня в номере университетской гостиницы недалеко от университета. Поскольку свободного времени у меня было довольно мало – всего два выходных, то и охватить все прелести этого островного государства мне, конечно, не удалось. На что я обратил внимание, помимо традиционно отмечаемой чистоты улиц и того, что за брошенный на дорогу окурок, можно угодить в тюрьму? (Правда, последнего я не смог проверить, так как сам то не курю…) Зато видно, что абсолютное большинство этого китайского анклава-китайцы, причем часто я встречал таких миниатюрных китайских студенточек, что их можно было бы вполне принять за куколок. Еще одно наблюдение – это асфальтовые дорожки для пешеходов (студентов), которыми они идут под крышей, защищая этот народ от муссонных, наверное, дождей. Напомню, что Сингапур лежит почти-что на самом экваторе –поэтому там весьма жарко и влажно. В столовой университета вам предлагаются 4 вида кухни: китайская, малайская, индийская и европейская. Сначала я решил попробовать индийский вариант, но быстро отказался – это почти чистый перец с небольшой добавкой карри и овощей. Поэтому я полностью отказался от экзотики и перешел на европейскую кухню. В городе-стране тоже есть деление на разные районы – китайские, индийские и малайские. Не упустил я и случая прокатиться на велорикше, что по цене конечно намного дороже, чем на автомобильном такси, да еще и сам человек рассказывает тебе на ломаном английском что-то о городе, правда, понять это почти невозможно. В индийском квартале приобрел небольшие отрезки натурального шелка для своих женщин (дочки и внучки) в России. (Они потом, вроде, даже что-то из этих тканей себе сшили). Из музеев посетил зоосад, но ... птиц. Жаль только, что красавцы фламинго дискредитировали себя ужасным запахом гуано. Попугай что-то сказавший по-китайски, вызывал бурные аплодисменты на трибунах, полных китайцами же... В последние выходные съездил на местный пляж, который находится в бухте Желтого Моря – вода там довольно мутная и теплая, как парное молоко. Сидя, конечно же, под тентом, наслаждался поеданием мороженного, похожего на наше – стандарт. Перед отъездом меня пригласили организаторы моего визита в ресторанчик за городом. Он был расположен среди очень тропических банановых деревьев, а что мы ели, я уже не помню, но не экзотику.

7. Издательская деятельность и локальные поездки

В 2008 г. вышел первый учебник по читаемому мной курсу – “Основы криптографии”. Соавтором был мой заведующий кафедрой В.П.П., который ввиду своей занятости бизнесом не мог, конечно, уделять много внимания

написанию этой книги, но организаторская его роль в этом вопросе была весьма велика. Чтобы сразу покончить с описанием издания этого учебника, скажу тут же, что второе издание его вышло в 2014 г., а третье – в 2016 г. при полноправном соавторстве моего ученика и коллеги по кафедре профессора В.А. Яковлева. Отмечу, правда, что статус этой книги был “учебное пособие”, хотя такая “кличка” объяснялось только тем, что он не получил гриф Министерства образования, как учебник для всех Вузов связи РФ. И, наверное, это было правильно не навязывать другим ВУЗам нашу книгу, хотя слово “пособие”, конечно, умаляло вес книги и резало глаз. Третье издание книги вышло в более солидном издательстве “Интермедиа” и было значительно лучше по полиграфии, за исключением контрастности текста я вообще оцениваю эту книгу достаточно высоко. Мне она казалась “эстетической”, поскольку, по определению М. Гемстергеймса, эстетическое – это то произведение, в котором вкладывается “максимальное количество информации при минимальном объеме средств представления”. И действительно, в этой книге я почти не добавил что-то абсолютно нового от себя, но потратил много времени и умственных сил, чтобы собрать и обработать все материалы по криптографии из известной мне открытой литературы. При написании ее передо мной постоянно стоял вопрос – доказывать что-либо строго или нет, сославшись на источник, где это уже было сделано? Все-таки мне хотелось, чтобы читатели не чувствовали себя недостойными полного понимания вопросов криптографии, которое требует изложения доказательств. С другой стороны, криптография – это точная наука, требующая для полного ее понимания хорошего знания специального математического аппарата и, главное, некоторой математической культуры, которая может быть и не у всех студентов обычных технических университетов. Впрочем, опыт преподавания данного предмета именно по этой книге в течение нескольких лет показал мне, что весь материал ее может быть успешно усвоен обычными студентами Бонча, но, конечно, требует от них определенного умственного напряжения.

В 2011 г. меня пригласили на 5 недель в Варшавский политехнический университет прочитать там лекционный курс “Foundation of Information Hiding”, причем деньги на это выделил Евросоюз. Конечно, меня в этом Евросоюзе не настолько знали, чтобы специально под меня выделять деньги. Просто предполагалось, что приглашение иностранных специалистов – это нормальная практика для улучшения процесса обучения в любом цивилизованном государстве. А в том факте, что именно я попал под этот проект, была значительная заслуга моего знакомого – доцента этого университета, о котором я уже писал раньше. Правда, я оказался не одним из приглашенных иностранных профессоров, о чем свидетельствовали объявления, вывешенные в фойе университета. Мой курс был представлен как семестровый спецкурс, который обеспечивал прослушавшим его студентам определенное количество credit hours. Записалось на этот курс всего порядка 15-20 студентов, что, возможно, объясняется отсутствием предварительной рекламы. Кроме того, как я обнаружил потом, у преподавателей кафедры, на которой этот курс читался, проявлялась некоторая ревность – мол, почему мы “не сами с усами”, хотя, конечно, нужно было бы

им признать, что в то время в Польше не было специалистов высокого уровня по данному направлению. Правда, там был один профессор Sz., но он специализировался в небольшой подобласти – сетевой стеганографии. Мне также рассказывали знакомые, что Pan Prof. Sz. упоминал, что заняться вопросами информационной безопасности подтолкнули его именно мои лекции и семинары, которые я проводил несколькими годами раньше в Государственном институте связи “Na Miedzeszine”.

Лекции в Варшаве пошли обычным порядком по 6-8 часов в неделю. К этому времени я уже привез с собой полный курс лекций, набранный на English для представления на компьютерном проекторе. Среди слушателей мне запомнилась одна симпатичная польская девушка (в интересном положении), которая довольно внимательно относилась к моему курсу и с которой мы иногда после лекций говорили на бытовые темы и один из иностранцев (вроде бы из Африки), который задавал мне множество вопросов.

Поселили меня в университетской гостинице в довольно небольшой комнате, однако, мне она вполне подходила. Свободное владение польским языком позволяло мне посещать галереи, музеи, концерты и т.п., не говоря уже о постоянном посещении уютного кафе на Nowym Swiate. Кроме того, я часто посещал своих знакомых (которые и способствовали пропаганде моих лекций) и имели, как я писал уже раньше, семь котов. Эта семья иногда приглашала меня в поездки на их машине. Так мы посетили мемориальное кладбище советских воинов в Варшаве и место рождения Ф. Шопена в Желязовой воле.

В один из выходных дней я осуществил свою давнюю мечту, будучи в Варшаве, на один день посетить Вену, благо что поезд идет туда всего одну ночь. Все это и произошло достаточно просто. Подошел на центральном варшавском вокзале к кассе, купил билет до Вены, показав свою Шенгенскую визу, вечером сел в купейный вагон, а утром вышел … на Венском вокзале. Самое удивительное, что тут я, наконец, почувствовал себя “Человеком мира” и не в том смысле, что меня все знают, а в том, что я могу ездить куда хочу и когда захочу, никого не спрашивая – мог ли я себе такое представить, находясь почти “невыездным” в России? (Так что не зря я выходил в 1991 г. строить баррикады на Исаакиевской площади. Свобода выезда из России, зафиксированная в конституции РФ – это замечательно!)

В Вене я посетил два больших музея, в которых были выставлены достаточно редкие для меня картины (Г. Климт, Шелле и др.), а также дворец Императоров Габсбургов. Потом меня вдруг понесло в ихний парк культуры и отдыха (Prater) с колесом обозрения, на которое я таки забрался, чтобы посмотреть на Вену свысока. Тут же зашел в ресторанчик, где в меню для еды были предложены всякие экзотические животные, вроде кенгуру, страусы и т.п., но я на это не решился, а заказал обычный бифштекс, который оказался, как всегда (вне Аргентины, наверное), подошвообразным. Еще мне удалось попасть на выездку дрессированных лошадей в Королевском Манеже – увы это было на уровне нашего выездного шапито. На сладкое зашел в знаменитое венское кафе, где делают еще более знаменитые венские пирожные Karscher. Последние показались мне даже ниже уровня нашего “Севера”, а кофе был хорош! Конеч-

но, не миновал я и квартиру-музей Моцарта – она оказалось очень скромной. Там же небольшой камерный квартет исполнял некоторые его произведения. Промучившись на вокзале, куда я приехал слишком загодя, уехал на поезде в Варшаву. Но ужас случился чуть позже! Сосед по тесному купе храпел всю ночь так, что стены вибрировали. Так что заснуть было невозможно – может это была месть за свержение Лжедмитрия в Смутное время?

В Польше в этот раз я почти согласовал с местным издательством предложение издать на польском языке, с переводом моим приятелем А.К. (из Политеха) моей книги “Основы криптографии”, изданной недавно в России. Увы, ничего из этого предложения не вышло – даже не помню сейчас в чем была причина. Но как-то не срослось...

Незаметно пробежали три года в Питере, где я много работал над статьями и докладами со своими аспирантами и вел курсы по криптографии и стеганографии для студентов. (Последний курс читал даже на английском языке для приглашенных на семестр в Бонч французских студентов.) Потом при поддержке профессора кафедры университета в Хельсинки, договорился прочитать мой любимый курс “Information Hiding”, что и сделал в течение четырех недель в Хельсинки в 2014 г. Познакомился там с одним финским профессором T. Karvi (по-русски, просто – Журавлев), которого позже пригласил к нам в Бонч прочитать лекцию о проверке секретности криптографических протоколов. Однако, это интересное направление, к сожалению, у нас в Бонче никто не подхватил.

Летом 2014 г. на меня напала серьезная хворь. Анализ ПСА показал значительное превышение нормы. Предложили сделать и позже выполнили две простые операции с брахитерапией. Все прошло благополучно и мне тогда даже разрешили поехать в Хельсинки.

Отмечу, что этот город мне всегда очень нравился. Хотя он и не претендует на помпезность некоторых европейских столиц, таких как Вена, Рим, Мадрид или даже Стокгольм. Я несколько раз бывал в нем на научных конференциях из серии FRUCT. Один раз мы с женой съездили туда просто так, для отдыха, заказав заранее билеты на интересный концерт в Дом музыки. Попутно сплавали на остров “Suomenlinen” и съездили в небольшой городок Porvoo в 50 км от Хельсинки. Любовались цветением сирени в парках и вдыхали ее запах – здесь еще не извели его из-за боязни аллергии. Мне нравилось жить в гостинице-башне “Toolo” – почти в центре, недалеко от вокзала и университета, в шаговой доступности до магазинов, порта и рынка; в последнем всегда можно было вкусить морепродукты за умеренную плату. Как-то мы с женой съездили даже в Стокгольм на огромном пароме (шесть этажей с лифтом) из класса “Silvia line”. Стокгольм нам тоже понравился – парадный и музейный, а также и со множеством воды снаружи и внутри. Интересен был музей “Одного корабля” – старинного галеона, извлеченного в наше уже время из воды и реставрированного. Правда, мы в этом городе чуть не опоздали на обратный рейс, так как там оказалось слишком много морских причалов.

В 2017 г. ко мне в аспирантуру поступил вьетнамец Нгуен (говорят, что большинство вьетнамцев тоже Нгуены...) Сначала я отнесся к этому аспиранту

подозрительно, поскольку он не очень владел английским и почти не владел русским. Что же касается стеганографии, то, конечно, он о ней не имел никакого “зеленого“ понятия. Правда, тему я ему дал довольно выигрышную, которая была посвящена совершенно новому (я бы сказал даже “асимметричному” методу обнаружения стегосистем), который я предложил пару лет назад, но пока он находился в очень сыром виде. Идея состояла в том, что обнаруживать СГ не обязательно по статистическим отличиям стеганограммы и покрывающего объекта, а можно только лишь по хорошим статистическим свойствам самой стеганограммы, если сообщение перед вложением подвергалось стойкому шифрованию и был известен метод извлечения сообщения из СГ. Это направление Нгуен проработал весьма подробно. Изучил эффективность для различных методов вложения, которая оказалась достаточно высокой. Дополнительно проработал и метод защиты от такого способа обнаружения при помощи дополнительного преобразования зашифрованного сообщения. Мы с ним также опубликовали по этому поводу несколько статей в отечественных и зарубежных журналах и в известиях научно-технических конференций [21]. Так что менее чем за три года был получен весь материал, необходимый по требованиям ВАК, для подобного рода кандидатских диссертаций. Такую диссертацию он и защитил успешно до окончания даже срока своей аспирантуры. Вот только эпидемия ковида немного задержала его возвращение на родину. Однако, в конце концов все кончилось благополучно, и он получил государственный диплом кандидата технических наук. Я всегда ставил Нгуена в пример некоторым другим моим аспирантам, которые, как правило, не укладывались в ранее согласованные сроки, да еще объясняя это мне тем, что они еще-де и работают... Правда, последнее я почти всегда квалифицировал, как “пьянство за рулем”, которое не смягчает, а усугубляет вину за ДТП. Вот так и надо работать и нашим аспирантам и тогда хвосты по защитам, даже уже выполненных работ, не будут растягиваться на годы!

К этому периоду (то есть 2014-2017 гг.) относятся публикации второго и третьего издания “Основ криптографии” и двух монографий по стеганографии (части 1 – собственно по СГ и части 2 – по ЦВЗ). В течение боле чем двух лет, я готовил материал для учебника по цифровой стеганографии, который правда должен выйти только в конце 2022 г. в одном из московских издательств и в соавторстве с моим завкафедры А.В.К., причем это был отнюдь не жест подхалимажа. Разделы, написанные моим соавтором, были посвящены сетевой СГ, то есть такой модели, когда для вложения используются свойства сетевых протоколов. Эта часть СГ была мне совершенно не известна, тогда как мой соавтор достаточно много занимался этим направлением, а, с другой стороны, это направление оказалось весьма востребованным для обеспечения информационной безопасности и поэтому его присутствие в нашем учебнике было более чем уместным.

Хотелось бы отметить, что не всегда нам удавалось беспрепятственно публиковать наши результаты в иностранных изданиях. Так в 2016 г. китайские ученые опубликовали в престижном международном журнале “Transaction on Information Forensics and Security” статью, в которой они предлагали произво-

дить распределение секретных ключей по каналам связи при помощи своей схемы EVSKey, и она, будто бы, обеспечивала их секретность при наличии перехвата. Прочитав эту статью, мы обнаружили, что авторы не учли одного метода извлечения ключа, который полностью компрометирует данную систему. Вскоре мы написали в раздел “Letters” этого журнала краткое сообщение под заголовком “Breaking of EVESKey Scheme”. Каково же было наше удивление, когда мы получили отказ от публикации в этом журнале на основании двух из трех отрицательных рецензий, авторы которых утверждали, что мы показали компрометацию этой схемы только при отсутствии шумов в канале перехватчика. Наш ответ на рецензию, где мы доказывали еще раз, что схема оказывается несекретной при тех же мощностях шумов в канале перехвата, что и легальном канале, не привел к допущению нашей статьи к ее публикации. Более того, почти такой же ответ мы получили и из журнала “Entropy” и почти с теми же несерьезными аргументами, хотя, казалось бы, что более страшного может быть для статьи, где декларируемая секретность демонстрируется как общедоступность? В конце концов, факт взлома данной схемы мы позднее опубликовали в нашей главе книги [20].

После 2014 г. я уже не пытался читать спецкурсы лекций за границей, сосредоточившись на публикации статей в отечественных и международных журналах, а также в подготовке и представлении докладов на отечественных и международных конференциях. При этом сохранял свои предыдущие научные направления – распределение ключей по каналам связи, стеганографию и цифровые водяные знаки. Типичными были такие мои работы как [21, 22]. Особо хочу сказать пару слов по работе [22]. Мне кажется, что там был изложен новый и достаточно необычный результат, который состоял в том, что по обычному бесшумному каналу связи (типа Интернета) можно достаточно просто выработать общий ключ недоступный для перехвата, причем такая задача вполне выполнима и для обычных пользователей (считай “чайников”). Важно, что такой подход не требует никаких, так называемых, “криптографических предположений”, которые используются в криптосистемах с открытым ключом (факторизация чисел, дискретное логарифмирование и т.п.) Что же касается международных конференций, где я выступал с докладами, то среди них можно отметить такие форумы как IISA-2015, CCEET-2016, Int. Journ. of Control Theory and Application-2017, SPIT-2017, MIPRO-2021, CNCrypt-2020, FRUCT-2017, 2018, 2019, FedCSIS-18, 19, 20. На последней конференции я неоднократно был членом программного комитета, мои работы (с соавторами) неоднократно отмечались, как лучшие. Наконец, в 2021 г. я был выбран, как FedCSIS General Chair, и что из этого получилось – полное фиаско. Я представил на последнюю конференцию неплохой совместный доклад, и будучи даже председателем, получил извещение о том, что наш доклад должен бать сокращен от Full до Short, причем, безо всякого объяснения причин? Конечно, мы от такого “харакири” отказались, и я вообще прекратил общение с организаторами этой конференции, несмотря на мою привязанность к Польше, где часто проводились ее заседания. Кстати, одно из заседаний конференции FedCSIS проводилось ранее в польском городе Гданьске. Этот старинный город несколько раз переходил от

одной страны к другой. Во время Великой отечественной войны он был почти полностью разрушен, и теперешняя историческая часть города представляет собой неплохой, правда, “новодел”. После окончания конференции я решил провести свой очередной “бросок” в соседнее государство, и, в частности, в Берлин, где я до сих пор еще не был. Правда, на этот раз я заказал там отель в центре, что дало мне возможность пробыв в Берлине целые сутки, посетить там несколько музеев, но, увы, не Рейхстаг, для посещения которого требовалось заранее записаться не позже чем за месяц до посещения. Еще одной моей мечтой была знаменитая улица Западного Берлина – Фридрихштрассе. Во времена присутствия Берлинской стены она была недоступной для туристов из СССР. Теперь же я смог свободно пройти туда пешком и даже посетить один из расположенных на ней ресторанов. Велико же было мое разочарование относительно обслуживания в этом ресторане, и качества бифштекса.

Помимо посещений разных стран в процессе, так сказать, научной работы, мы с женой иногда совершали чисто отдыхательные вояжи. Помимо упоминавшихся уже поездок в Хельсинки и Стокгольм, нам удалось съездить в Финляндию (в Новый Валаам), где находится спасенная в 1939 г. Валаамская икона Богородицы. Мы были там крепкой зимой и поэтому наслаждались красотой зимних пейзажей и свободным посещением нововалаамского храма. Ещё одно погружение на Север мы совершили, когда посетили городок Pello за Полярным кругом в Финляндии, для чего нам пришлось ехать целую ночь из Хельсинки на север на поезде. Наслаждались там полным отсутствием туристов (в отеле мы жили вдвоем и, несмотря на это, нам там каждое утро специально готовили завтраки). В отличие от ожидавшейся чахлой тундры, мы встретились здесь с лесисто-холмистой местностью и идеально белым снежным покровом, как на природе, так и в поселке. Подъехав на … такси до лыжно-снегоходной базы, но уже в Швеции, мы там арендовали лыжи и чуть было не заблудились в бескрайних снежных просторах, избежав слалома на местных холмах, только из-за временного закрытия подъемников. Переехав замершую широкую реку, мы оказались снова в гостеприимной Финляндии. (Вспомнилась песня Покраса, написанная им в СССР перед Зимней войной 1939-1940 гг. – “Принимай нас Суоми красавица с голубыми глазами озер...”).

Летом 2020 г. меня ожидало еще одно испытание моего здоровья. А именно после службы в Зеленогорской церкви, летним днем 2020 г. я почувствовал, направляясь к выходу, что что-то со мой не так – когда сидишь или даже просто стоишь не двигаясь, то все хорошо, но стоит сделать хотя бы один шаг или поднять руку, то сразу начинает казаться что сейчас ты потеряешь сознание и упадешь. Измерил частоту пульса – 30 уд/мин ... разве при таком пульсе люди еще живут?! Поддерживаемый женой и экономя силы для каждого шага, я с трудом добрался сначала до скамейки рядом с храмом, а потом и до моего автомобиля, стоявшего примерно в 100 м. Попытался сесть за руль и завести мотор, а потом поехал, стараясь не делать лишних телодвижений. Так удалось потихоньку проехать 30 км до моей дачи. Пульс стойко показывал 30. Вызвали скорую помощь. Приехала симпатичная девушка, которая предложила госпитализацию (спасибо ей и пришедшей соседке по даче Г., которая тоже это

решение поддержала). Потом два часа езды с сиреной до города. Час ожидания в подвале среди других больных на каталках и заезд в больничную палату. Через пару дней был консилиум пары д.м.н. и предложение поставить кардиостимулятор, что было мною принято и осуществлено хирургом в тот же день. Затем еще несколько дней на реабилитацию и возвращение домой, как я теперь говорю "с железякой в сердце". Пришлось привыкать к новой реальности. Теперь приходилось выбирать маршруты метро с отсутствием или с небольшими по длине ступенчатыми переходами, избегать подъемов на этажи без лифтов, не носить больше 5 кг в руках, отказаться от лыжных прогулок на липком снегу, а главное, ходить медленно (жена называла это "пыточным шагом"). И раз в год приходить на remote control, когда медик-компьютерщик дистанционно регулирует твою жизнь, положив свой датчик тебе на грудь. Ну что же, и к этому можно было привыкнуть. Хорошо еще, что это произошло еще до санкций и мне поставили двухкамерный американский кардиостимулятор. Ну, а в остальном, можно было продолжать жить, как обычно. (Вспоминается персонаж романа М.С. Степновой "Женщины Лазаря", где главный герой, академик, уже совершенно обессилевший и непригодный к семейной жизни (у меня-то было не так…), все еще пишет статьи, руководит аспирантами и даже … надеется на "Нобелевку".)

Вместо заключения: 85 лет – краткие итоги

В августе 2021 г. мне исполнилось … аж 85 лет. Говорят, что это не юбилейная (так как не круглая) дата. Но не только поэтому мы с М. отметили ее достаточно скромно – посетили литургию в зеленогорской церкви (где, кстати, настоятель – отец В. в этот день всегда отмечает свою интронизацию). Потом проехали в один из ресторанчиков на берегу Финского залива, чтобы там просто вкусно поесть без выпивки (так как я был за рулем) и, наконец, отправились к себе на дачу, чтобы уж там восполнить последний пробел. Но много позднее, когда уже начался учебный процесс в Бонче, пришлось отдать дань и коллективному празднику. (Правда, еще пред этим, на первом в этом учебном году собрании преподавателей Бонча, ректор меня поздравил и вручил ведомственную медаль "100 лет службе шифрования и криптографии РФ", присланную мне из Москвы вместе с наградным удостоверением, подписанным соответствующим генералом. Конечно, я понимал, что это не государственная награда, но, все-таки, было приятно – ведь я много сил и научных трудов отдал некоторым (хотя и не главным, наверное) проблемам этой науки. Местное мое чествование (с банкетом) состоялось в ноябре того же года в университетской столовой. Собралось человек 40 в основном из Бонча, но пришли и некоторые мои знакомые и ученики из других организаций, или просто … сошли с пенсионных диванов. Для начала, краткое мое жизнеописание озвучил мой ученик В.А.Я. Потом приступили к трапезе и выпивке под аккомпанемент коротких спичей. Это была для меня самая трудная часть – выслушивать всякие похвалы в мою честь. Но тут никуда уж не денешься – хуже было бы если бы вместо этого произносилась бы сплошная хула, хотя именно так славили в Древнем Риме провозимого по улицам вечного города военноначальника, признанного три-

умфатором. (Кстати, более подробно о моей биографии и научных трудах можно прочитать в журнале “Труды учебных заведений связи”, № 3 за 2021 год.)

Юбилейное мероприятие дало мне повод еще раз задуматься над итогами моей профессиональной деятельности. Конечно, сам я не могу себя отнести к первому ряду мировых и даже отечественных ученых в области теории связи или информационной безопасности. Но, видит Бог, я старался что-то сделать в науке и в обучении и, прежде всего, потому, что это было мне самому интересно. Мне страшно повезло, что работа была для меня не только средством для обеспечения моего существования и существования моей семьи, но и средством получать от всего этого удовольствие. Конечно, надо было потратить много сил и времени, чтобы написать около 200 печатных работ, среди которых 20 монографий и учебников, а сколько энергии и усидчивости надо было потратить на подготовку и успешную защиту 38 моих учеников (адъюнктов и аспирантов!), причем среди них не было ни одного человека, который бы не прошел вместе со мной весь цикл – от выбора темы до написания научных работ и глав диссертации, а также нелегкую процедуру подготовки к защите. Не буду перечислять даже мои основные научные результаты, но упомяну лишь некоторые из них, которые мне казались особенно важными. Такие, например, как:

- границы для обнаружения и исправления ошибок в каналах со случайной структурой;
- формула для оценки утечки информации к перехватчику в отводном канале;
- определение огибающей сигнала и расширенного преобразования Гильберта;
- обобщенная теорема усиления секретности;
- стеганография в каналах с шумом;
- обнаружение СГ при шифровании сообщений;
- распределение ключей по каналам связи с различными свойствами.

Своей заслугой я считаю также постановку лекционных курсов по кодированию в каналах со случайной структурой, курсов по основам криптографии и стеганографии для инженерных ВУЗов. Сбылась моя еще студенческая мечта посетить различные страны, причем не только (и не столько!) как турист или “на танке”, но и как преподаватель и научный работник, что конечно обеспечило мне большее проникновение в культуру и быт различных стран. Немного я занимался также и любительским спортом (теннис, лыжи, туризм), что добавляло мне энергии в нахождении после этого новых интересов в науке и образовании.

Какие вопросы по моим направлениям кажутся мне наиболее актуальными для дальнейших исследований?

По криптографии:

- распределение ключей по различным каналам связи с шумами и без них;
- аутентификация пользователей при распределении ключей;

– различные криптографические протоколы (совместные секретные вычисления, тайное голосование и др.);
– криптосистемы с открытым ключом на основе использования решеток;
– протоколы квантовой криптографии, устойчивые к полупрозрачным атакам.

По стеганографии и системам с ЦВЗ:

– стегосистемы “без погружения” (generative adversarial network-GAN), которые начали развиваться в последнее десятилетие, но до сих пор они еще недостаточно проработаны;
– распределение ключей по каналам связи с использованием методов стеганографии.

Конечно, за последние несколько лет мне пришлось несколько умерить свою активность. Перейдя на позицию “Почетного профессора Бонча”, я смог освободиться от рутинного потока занятий, ограничившись чтением только отдельных лекций, руководством аспирантами, публикацией учебников и научных работ. (Так за последние 5 лет я опубликовал порядка 15 печатных работ в журналах из перечня ВАК и индексированных в Scopus и Web of Science, выступил с докладами на 15 международных конференциях, издал (в соавторстве) 2 монографии и почти издал фундаментальный учебник по стеганографии, который должен выйти в ближайшее время, выпустил трех аспирантов, участвовал в работе, как член трех диссертационных советов. Не могу, правда, поставить только себе в полную заслугу тот факт, что у меня 7 внуков, некоторые из которых окончили уже или учатся в различных университетах. На каникулах езжу на своей машине на дачу, где зимой катаюсь на лыжах, а летом немного ухаживаю за садом, купаюсь в местных озерах, собираю в лесу ягоды и грибы, иногда рыбачу в ближайших озерах. Надеюсь, что мой опус может способствовать научным работникам в понимании того, что научную и педагогическую деятельность, можно успешно совмещать с посещением зарубежных стран, наблюдением природы и любительским спортом.

В общем, слава Богу за все!

Литература

1. Klove T. Generalization of the Korzhik bound // IEEE Trans. Inform. Theory. 1984. № 30. p. 771-773.

2. Коржик В. И., Финк Л. М. Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой. – М.: Связь, 1975.

3. Коржик В. И., Финк Л. М., Щелкунов К. Н. Расчет помехоустойчивости цифровых сигналов. Справочник. – М.: Радио и Связь, 1981.

4. Wyner A. The wire-tap channel // Bell Syst. Tech. J. 1975. № 8.

5. Diffie W., Hellman M. New directions in cryptography // IEEE Trans on IT. 1976. № 22. p. 644-654.

6. Korzhik V., Turkin A. Cryptanalysis of McElice public-key cryptosystem // Proc. of Eurocrypt’91. 1991. p. 68-70.

7. Zastosowanie metod kryptografichnych dla zapewnienia bezpiechenstwasieci komputerowych. – Warsaw, Telecommunication Institute Publisher, 1996, 120 p. (in Polish).

8. Korzhik V., Barg A., Henk van Tilborg A broadcast key distribution scheme based on block designs // 5-th IMA Conference, Proc. in Lecture Notes in Computer Science. № 1025. – Chirencester, 1995. – P. 2-12.

9. Menezes A., Oorshot P., Vanstone S. Handbook of applied cryptography. – CRC, 1997.

10. Schneier B. Applied Cryptography. – W and S, 1994.

11. Korzhik V., Luna G.M., Balakirsky V. Privacy amplification theorem for noisy main channel // International Conference “Information Security”. Lecture Notes in Computer Science, vol. 2200 – Spain, 2001. P. 18-26.

12. Korzhik V. et al. A performance Evaluation of Digital Watermark Under an Additive Noise Attack Condition // Proceedings VII Spanish Meeting on Cryptography and Information Security-2002. – Spain, 2002. – P. 451-470.

13. Korzhik V., Lopato Yu. Noise-immune coding when using modems with decision feedback // Telecommunications and Radio Engineering, part 1. 1971. Vol. 43. № 8. P. 29-36.

14. Korzhik V., Lee M.H. Image Authentication Based on Modular Embedding // IEICE Trans. on IT and Systems. 2006. Vol. E89. № 4. pp. 1498-1506.

15. Korzhik V., Lee M.H. On the Existence of Perfect Stegosystems // IWDW’2005, Lecture Notes in Computer Science. 2005. Vol. 3710. p. 30-37.

16. Korzhik V., Loban K., Luna G. M. Undetectable Spread-time Stegosystem Based on Noisy Channels // International Journal of Computer Science and Applications, Special Issue on Multimedia application. 2011. Vol. VIII. № 1.

17. Korzhik V., Luna G.M., Yakovlev V. Key Distribution Protocols Based on Noisy Channels in Presence of an Active Adversary: Conventional and New Versions with Parameter Optimization // Trans. IEEE on IT, Special Issue on Information Security. 2008. Vol. 54. № 6. pp. 2535-2550.

18. Korzhik V. et al. Secret Key Agreement Over Multipath Channels Exploiting Variable-Directional Antenna // International Journal of Advanced Computer Science and Applications. 2012. № 1.

19. Тихонов С. В., Коржик В. И. Методы защиты аппаратной реализации шифра ГОСТ от атаки измерения потребляемой мощности в цепи питания // Проблемы информационной безопасности. Компьютерные системы. 2013. № 3. С. 62-72.

20. Korzhik V. et al. Advance in Keyless Cryptography / Chapter in the book Modern Cryptography. – Inteltech, 2022.

21. Korzhik V. et al. Side Attacks on Stegosystems Executing Messages Encryption Previous Embedding // Journal of Information Hiding and Multimedia Signal Processing. 2020. vol. 11. № 01. p. 44-58.

22. Korzhik V. et al. Protocol of key distribution over public noiseless channels executing without cryptographic assumption // International; Journal of Computer Science and Application. 2020. vol. 17. № 01. p. 1-14.

References

1. Klove T. Generalization of the Korzhik bound // IEEE Trans. Inform. Theory. 1984. № 30. p. 771-773.

2. Коржик В. И., Финк Л. М. Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой. – М.: Связь, 1975.

3. Коржик В. И., Финк Л. М., Щелкунов К. Н. Расчет помехоустойчивости цифровых сигналов. Справочник. – М.: Радио и Связь, 1981.

4. Wyner A. The wire-tap channel // Bell Syst. Tech. J. 1975. № 8.

5. Diffie W., Hellman M. New directions in cryptography // IEEE Trans on IT. 1976. № 22. p. 644-654.

6. Korzhik V., Turkin A. Cryptanalysis of McElice public-key cryptosystem // Proc. of Eurocrypt'91. 1991. p. 68-70.

7. Zastosowanie metod kryptografichnych dla zapewnienia bezpiechenstwasieci komputerowych. – Warsaw, Telecommunication Institute Publisher, 1996, 120 p. (in Polish).

8. Korzhik V., Barg A., Henk van Tilborg A broadcast key distribution scheme based on block designs. *5-th IMA Conference, Proc. in Lecture Notes in Computer Scienc*, 1995, no. 1025, pp. 2-12.

9. Menezes A., Oorshot P., Vanstone S. *Handbook of applied cryptography*. CRC, 1997.

10. Schneier B. *Applied Cryptography*. W and S, 1994.

11. Korzhik V., Luna G. M., Balakirsky V. Privacy amplification theorem for noisy main channel. *International Conference "Information Security". Lecture Notes in Computer Science*, 2001, vol. 2200, pp. 18-26.

12. Korzhik V. et al. A performance Evaluation of Digital Watermark Under an Additive Noise Attack Condition. *Proceedings VII Spanish Meeting on Cryptography and Information Security-2002*, 2002, pp. 451-470.

13. Korzhik V., Lopato Yu. Noise-immune coding when using modems with decision feedback. *Telecommunications and Radio Engineering, part 1*, 1971, vol. 43, no. 8, pp. 29-36.

14. Korzhik V., Lee M.H. Image Authentication Based on Modular Embedding. *IEICE Trans. on IT and Systems*, 2006, vol. E89, no. 4, pp. 1498-1506.

15. Korzhik V., Lee M.H. On the Existence of Perfect Stegosystems. *IWDW'2005, Lecture Notes in Computer Science*, 2005, vol. 3710, pp. 30-37.

16. Korzhik V., Loban K., Luna G. M. Undetectable Spread-time Stegosystem Based on Noisy Channels. *International Journal of Computer Science and Applications, Special Issue on Multimedia application*, 2011, vol. VIII, Issue 1.

17. Korzhik V., Luna G.M., Yakovlev V. Key Distribution Protocols Based on Noisy Channels in Presence of an Active Adversary: Conventional and New Versions with Parameter Optimization. *Trans. IEEE on IT, Special Issue on Information Security*, 2008, vol. 54. no. 6, pp. 2535-2550.

18. Korzhik V. et al. Secret Key Agreement Over Multipath Channels Exploiting Variable-Directional Antenna // International Journal of Advanced Computer Science and Applications. 2012. No. 1.

19. Tikhonov S., Korzhik V. Method of hardware implemented gost cipher protection against dpa and hodpa attacks. *Information Security Problems. Computer Systems*, 2013, no. 3, pp. 62-72 (in Russian).

20. Korzhik V. et al. *Advance in Keyless Cryptography*. Chapter in the book "Modern Cryptography". Inteltech, 2022.

21. Korzhik V. et al. Side Attacks on Stegosystems Executing Messages Encryption Previous Embedding. *Journal of Information Hiding and Multimedia Signal Processing*, 2020, vol. 11, no. 01, pp. 44-58.

22. Korzhik V. et al. Protocol of key distribution over public noiseless channels executing without cryptographic assumption. *International; Journal of Computer Science and Application*, 2020, vol. 17, № 01, pp. 1-14.

Статья поступила 20 июня 2022 г.

Информация об авторе

Коржик Валерий Иванович – доктор технических наук, профессор, заслуженный деятель Высшей школы РФ. Профессор кафедры информационной безопасности. Санкт-Петербургский государственный университет телекоммуникаций имени профессора М. А. Бонч-Бруевича. Область научных интересов: теория информации, концепция подслушивающего канала, прикладная криптография и стеганография. E–mail: val-korzhik@yandex.ru

Адрес: 191186, Санкт-Петербург, наб. реки Мойки, д. 61.

Valery Korzhik: Along the ways paved by Shannon, Fink and Wyner

V. I. Korzhik

"The main think is to do everything with a passion, it decorates life very much"
L. Landau

Actuality. *The description of scientific and teaching activity for doctor of technical science, Professor, honored worker of Russian Federation High School, honorary Professor of Saint-Petersburg State University named after M.A. Bonch-Bruevich (SUT), IEEE on IT Member Valery Korzhik is presented in the current paper. The main direction of his scientific activity are: signal theory, information theory, error correcting codes, information security including so called "keyless cryptography". His academic activity is divided in two parts: 25-years duration of his service in Military Communication Academy and Full Professor position in SUT from 1989 y. till now. Besides of them he was working as visiting Professor during three and half years at Mexican University "Cinvestav", also he took part in researches and teaching process at 15 Universities of Europe, USA, Asia and Australia. As the results of such research activity he was publishing in Russian and international scientific journals about 200 research papers including 20 monographs and text books (while one book is written in English and one in Polish) .He was a supervisor for more than 50 engineers and 38 candidates of technical science (Ph.D). Seven last have received later the degree of Doctor of Science and taken Professor positions in Russian or abroad. In the current paper are described also peculiarities of teaching at foreign Universities, nature and customs in countries where he was teaching students and collaborate with Professors.* ***The goals of paper*** *is to show that every motivated and successful Russian*

scientist be manage to combine his research and academic activity and collaboration with foreign scientists executing such travelling process with more stronger motivation of his research work in order to avoid too tedious professional discussion it was added into the paper some remarkable stories from author's life during his travelling over the world. ***Practical importance*** *of the current paper is to specify for young scientists the important problems in area of information security and make sure for them that contacts with similar researches over the world can result in a power motivation to be always capable to solve them.*

Key words: *information theory, wire-tap channel concept, applied cryptography and steganography, specific academic activity abroad.*

Information about Author

Valery Ivanovich Korzhik – Doctor of technical science, Professor, Honored worker of Russian Federation High School. Honorary Professor of Saint-Petersburg State University named after M.A. Bonch-Bruevich, IEEE on IT Member. Research interests: information theory, wire-tap channel concept, applied cryptography and steganography. E–mail: val-korzhik@yandex.ru

Address: Russia, 191186, Saint Petersburg, Moyka nab., 61.